(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-173285
(P2004-173285A)
(43)公開日　平成16年6月17日(2004.6.17)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/32	H04L	9/00	673A	5B085
G06F	15/00	G06F	15/00	330B	5J104
G09C	1/00	G09C	1/00	640E	
H04L	9/16	H04L	9/00	643	

審査請求 未請求　請求項の数 47　OL　（全 36 頁）

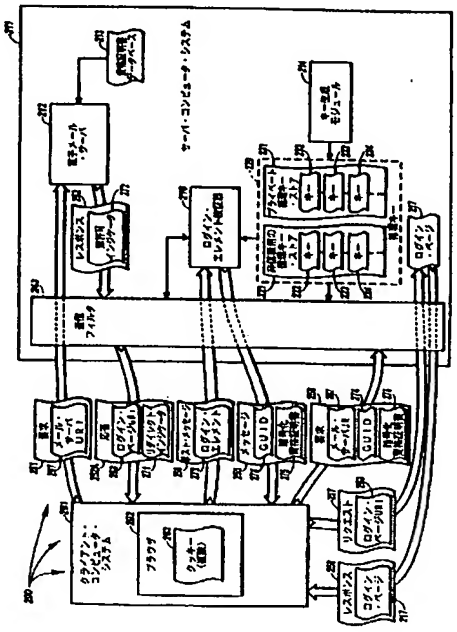
(21)出願番号　特願2003-391491(P2003-391491)
(22)出願日　平成15年11月20日(2003.11.20)
(31)優先権主張番号　60/428,152
(32)優先日　平成14年11月20日(2002.11.20)
(33)優先権主張国　米国(US)
(31)優先権主張番号　10/459,863
(32)優先日　平成15年6月12日(2003.6.12)
(33)優先権主張国　米国(US)

(71)出願人　391055933
マイクロソフト　コーポレイション
MICROSOFT CORPORATION
アメリカ合衆国　ワシントン州　98052-6399　レッドモンド　ワン　マイクロソフト　ウェイ　（番地なし）
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ショーン　デリク　ブレースウェル
アメリカ合衆国　98019　ワシントン州　ドボル　284　サークル　ノースイースト　14008

最終頁に続く

(54)【発明の名称】リソースへのウェブ・ベースのアクセスに使用されるクライアントの資格証明書の安全な処理

(57)【要約】
【課題】　リソースへのウェブ・ベースのアクセスに使用されるクライアントの資格証明書の安全な処理を提供すること。
【解決手段】　ユーザの資格証明書を入力するインターフェースを有するログイン・ページがクライアントで提示され、入力されたユーザの資格証明書がサーバに送信される。ユーザの資格証明書の受信に呼応して、サーバはクライアントに対する一意のセッションＩＤを生成する。サーバはまた循環鍵ストアの現在の鍵と一意のセッションＩＤとに基づいてユーザの資格証明書に対するデジタル署名を導出する。次いでサーバは現在の鍵と一意のセッションＩＤから導出された暗号鍵に基づいてデジタル署名とユーザの資格証明書とを暗号化する。暗号化された資格証明書がクライアントに返信されると、循環鍵ストアの鍵を使用して資格証明書の有効性確認を試みる。ユーザの資格証明書の有効性が確認不可であると、ユーザには再びログイン・ページが提示される。
【選択図】　図２Ａ



【特許請求の範囲】
【請求項１】
サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを試みるクライアント・コンピュータ・システムにおいて、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法であって、
前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第１の要求を送信する動作（act）と、
前記クライアント・コンピュータ・システムが、ユーザの資格証明書を受け入れるためのインターフェースを提供するログイン・ページにリダイレクトされる動作（act）と、
前記クライアント・コンピュータ・システムが、前記ログイン・ページを使用して、前記ユーザの資格証明書を前記サーバ・コンピュータ・システムに提出する動作（act）と、
前記クライアント・コンピュータ・システムが、提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は、前記提出されたユーザの資格証明書の少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は、暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を受信する動作（act）と、
前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記暗号化された情報をこの時点で含んでいる、第２の要求を送信する動作（act）と
を備えることを特徴とする方法。
【請求項２】
前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第１の要求を送信する前記動作（act）は、以前に受信した暗号化された情報と以前に受信した一意のセッションＩＤとを送信する動作（act）を備えることを特徴とする請求項１に記載の方法。
【請求項３】
前記クライアント・コンピュータ・システムが前記ログイン・ページにリダイレクトされる前記動作（act）は、前記サーバ・コンピュータ・システムによって前記以前に受信した暗号化された情報が有効であるとされなかった結果、前記クライアント・コンピュータ・システムが前記ログイン・ページにリダイレクトされる動作（act）を備えることを特徴とする請求項２に記載の方法。
【請求項４】
前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第１の要求を送信する前記動作（act）は、電子メール・サーバの電子メール・リソースへのウェブ・ベースのアクセスを求めるＨＴＴＰメッセージを送信する動作（act）を備えることを特徴とする請求項１に記載の方法。
【請求項５】
前記クライアント・コンピュータ・システムが、前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報を受信する前記動作（act）は、前記暗号化された情報を一意のセッションＩＤと共に受信する動作（act）を備えることを特徴とする請求項１に記載の方法。
【請求項６】
前記受信した暗号化された情報と前記受信した一意のセッションＩＤとを前記クライアント・コンピュータ・システムの対応するクッキーに記憶する動作（act）をさらに備えることを特徴とする請求項５に記載の方法。
【請求項７】
前記クライアント・コンピュータ・システムが、前記リソースへのウェブ・ベースのア

クセスを求める第２の要求を送信する前記動作（act）は、前記暗号化された情報を一意のセッションＩＤと共に送信する動作（act）を備えることを特徴とする請求項１に記載の方法。

【請求項８】

前記クライアント・コンピュータ・システムが、前記ログイン・ページを使用して、ユーザの資格証明書を前記サーバ・コンピュータ・システムに提出する前記動作（act）は、前記クライアント・コンピュータ・システムが、前記ログイン・ページを使用して、ユーザの資格証明書を安全な相互に認証された接続を介して前記サーバ・コンピュータ・システムに提出する動作（act）を備えることを特徴とする請求項１に記載の方法。

【請求項９】

サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求をクライアント・コンピュータ・システムから受信する前記サーバ・コンピュータ・システムにおいて、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法であって、

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信された第１の要求を受信する動作（act）と、

前記サーバ・コンピュータ・システムが、前記第１の要求に呼応して、前記クライアント・コンピュータ・システムがユーザの資格証明書を入力することのできるログイン・ページに、前記クライアント・コンピュータ・システムをリダイレクトする動作（act）と、

前記サーバ・コンピュータ・システムが、前記ログイン・ページで提出されたユーザの資格証明書を受信する動作（act）と、

前記サーバ・コンピュータ・システムが、前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は、前記ユーザの提出した資格証明書の少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は、暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を送信する動作（act）と、

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信され、前記暗号化された情報を含んでいる、第２の要求を受信する動作（act）と

を備えることを特徴とする方法。

【請求項１０】

前記サーバ・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを求める第１の要求を受信する前記動作（act）は、以前に生成された暗号化された情報と以前に生成された一意のセッションＩＤとを受信する動作（act）を備えることを特徴とする請求項９に記載の方法。

【請求項１１】

前記サーバ・コンピュータ・システムが前記第１の要求に呼応してログイン・ページに前記クライアント・コンピュータ・システムをリダイレクトする前記動作（act）は、以前に生成された前記暗号化された情報が前記サーバ・コンピュータ・システムによって有効であるとされなかった結果、前記サーバ・コンピュータ・システムが前記クライアント・コンピュータ・システムをログイン・ページにリダイレクトする動作（act）を備えることを特徴とする請求項９に記載の方法。

【請求項１２】

前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第１の要求を受信する前記動作（act）は、電子メール・サーバの電子メール・リソースへのウェブ・ベースのアクセスを求めるＨＴＴＰメッセージを受信する動作（act）を備えることを特徴とする請求項９に記載の方法。

【請求項１３】
前記サーバ・コンピュータ・システムが、前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報を送信する前記動作（act）は、前記暗号化された情報を一意のセッションＩＤと共に送信する動作（act）を備えることを特徴とする請求項９に記載の方法。
【請求項１４】
前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める第２の要求を受信する前記動作（act）は、前記暗号化された情報を一意のセッションＩＤと共に受信する動作（act）を備えることを特徴とする請求項９に記載の方法。
【請求項１５】
前記クライアント・コンピュータ・システムから、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を受信するサーバ・コンピュータ・システムにおいて、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法であって、
前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムによって送信された第１の要求を受信する動作（act）と、
前記クライアント側の資格証明書がリソースへの無許可のアクセスを悪意のあるユーザに提供する可能性を低減するように、循環鍵ストアからの鍵を使用して前記クライアント側の資格証明書をセキュリティ保護する動作（act）と、
前記サーバ・コンピュータ・システムが、前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信された、暗号化された情報を含んでいる、第２の要求を受信する動作（act）と
を備えることを特徴とする方法。
【請求項１６】
クライアント・コンピュータ・システムにおいて、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスのために使用されるユーザの資格証明書を維持する方法であって、
前記クライアント・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを求める要求であって、前記要求は、一意のセッションＩＤとユーザの資格証明書の少なくとも一部および時間依存署名を表す暗号化された情報とを含み、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記要求を送信する動作（act）と、
前記ユーザの資格証明書の前記少なくとも一部とリフレッシュされた時間依存署名とを表すリフレッシュされた暗号化された情報であって、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部とリフレッシュされた署名時間依存鍵とから導出されており、前記暗号化された情報は、リフレッシュされた暗号化された時間依存鍵を使用して暗号化され、前記リフレッシュされた署名時間依存鍵と前記リフレッシュされた暗号化された時間依存鍵は両方とも循環鍵ストアの最新の鍵から引き出されている、前記リフレッシュされた暗号化された情報と更新された一意のセッションＩＤとともに前記要求されたリソースを、前記クライアント・コンピュータ・システムがクライアント側のブラウザで受信する動作（act）と、
前記クライアント・コンピュータ・システムが、前記更新されたセッションＩＤと前記リフレッシュされた暗号化された情報とをクライアント・コンピュータ・システムの対応するクッキーに記憶する動作（act）と
を備えることを特徴とする方法。
【請求項１７】

前記クライアント・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを求める要求を送信する前記動作（act）は、電子メール・サーバの電子メール・リソースへのウェブ・ベースのアクセスを求めるＨＴＴＰメッセージを送信する動作（act）を備えることを特徴とする請求項１６に記載の方法。

【請求項１８】

前記クライアント・コンピュータ・システムが、前記要求されたリソースを更新された一意のセッションＩＤとリフレッシュされた暗号化された情報と共にクライアント側のブラウザで受信する前記動作（act）は、前記暗号化された情報の生成で使用されている鍵が循環鍵ストアの前記最新の鍵でないということに起因して、更新されたセッションＩＤとリフレッシュされた暗号化された情報とを受信する動作（act）を備えることを特徴とする請求項１６に記載の方法。

【請求項１９】

前記クライアント・コンピュータ・システムが、前記更新された一意のセッションＩＤと前記リフレッシュされた暗号化された情報とを前記クライアント・コンピュータ・システムの対応するクッキーに記憶する前記動作（act）は、前記一意のセッションＩＤと前記リフレッシュされた暗号化された情報をブラウザ・メモリ内の前記一意のセッションＩＤと暗号化された情報に上書きする動作（act）を備えることを特徴とする請求項１６に記載の方法。

【請求項２０】

サーバ・コンピュータ・システムで、前記サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスに使用されるユーザの資格証明書の有効性を決定する方法において、

前記サーバ・コンピュータ・システムが、前記サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求であって、前記要求は、一意のセッションＩＤと、前記ユーザの資格証明書の少なくとも一部および時間依存署名を表す暗号化された情報とを含み、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記要求を受信する動作（act）と、

前記サーバ・コンピュータ・システムが、循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の少なくとも一部の有効性確認を試みる動作（act）と、

前記サーバ・コンピュータ・システムが、前記要求されたリソースへのウェブ・ベースのアクセスを制御するモジュールに前記要求を転送する動作（act）と、

前記サーバ・コンピュータ・システムが、前記ユーザの資格証明書の前記少なくとも一部と前記時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきか否かを判定する動作（act）と

を備えることを特徴とする方法。

【請求項２１】

前記循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の少なくとも一部の有効性確認を試みる前記動作（act）は、前記循環鍵ストアの前記最新の鍵に基づいて前記ユーザの資格証明書の前記少なくとも一部が有効であると判定する動作（act）を備えることを特徴とする請求項２０に記載の方法。

【請求項２２】

前記循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の前記少なくとも一部の有効性確認を試みる前記動作（act）は、前記循環鍵ストアの前記最新の鍵に基づいて前記ユーザの資格証明書の前記少なくとも一部が有効でないと判定する動作（act）を備えることを特徴とする請求項２０に記載の方法。

【請求項２３】

前記サーバ・コンピュータ・システムが、前記循環鍵ストア内の以前に生成された鍵で前記循環鍵ストア内に前記最新の鍵よりも前に挿入された鍵、に基づいて前記ユーザの資

格証明書の前記少なくとも一部が有効であると判定する動作（act）をさらに備えることを特徴とする請求項２０に記載の方法。

【請求項２４】

前記サーバ・コンピュータ・システムが、前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきか否かを判定する前記動作（act）は、前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきであると判定する動作（act）を備えることを特徴とする請求項２０に記載の方法。

【請求項２５】

前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されるべきであると判定する前記動作（act）は、前記サーバ・コンピュータ・システムが、前記循環鍵ストア内の以前に生成された鍵で、前記循環鍵ストア内に最新の鍵より前に挿入された鍵、に基づいて前記ユーザの資格証明書の少なくとも一部を有効であると判定する動作（act）を備えることを特徴とする請求項２４に記載の方法。

【請求項２６】

前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報とが前記循環鍵ストアの前記最新の鍵から導出されるべきであると判定する前記動作（act）は、前記サーバ・コンピュータ・システムが、前記循環鍵ストア内のいかなる鍵によっても前記ユーザの資格証明書の前記少なくとも一部を有効であるとすることができなかったと判定する動作（act）を備えることを特徴とする請求項２４に記載の方法。

【請求項２７】

前記サーバ・コンピュータ・システムは、ユーザの資格証明書を受信するためのインターフェースを提供するログイン・ページに前記クライアント・コンピュータ・システムをリダイレクトする動作をさらに備えることを特徴とする請求項２６に記載の方法。

【請求項２８】

前記サーバ・コンピュータ・システムが、前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されているか否かを判定する前記動作（act）は、リフレッシュされた暗号化された情報と時間依存署名とを前記循環鍵ストアの前記最新の鍵から導出する動作（act）を備えることを特徴とする請求項２０に記載の方法。

【請求項２９】

前記サーバ・コンピュータ・システムは、前記要求されたリソースと前記更新された一意のセッションＩＤとリフレッシュされた暗号化された情報とを前記クライアント・コンピュータ・システムに送信する動作（act）をさらに備えることを特徴とする請求項２８に記載の方法。

【請求項３０】

メッセージ・ヘッダーを変更することができる通信フィルタを含むサーバ・コンピュータ・システムにおいて、クライアント・コンピュータ・システムに関連付けられた通信プロパティを決定する方法において、

ＨＴＴＰメッセージの処理方法を変更することのできる１つまたは複数の選択可能な通信プロパティを選択するためのインターフェースを含むログイン・ページを前記クライアント・コンピュータ・システムに送信する動作（act）と、

前記ログイン・ページから選択可能な前記１つまたは複数の選択可能な通信プロパティで、前記クライアント・コンピュータ・システムとのＨＴＴＰ通信の処理方法を前記通信フィルタに指示する通信プロパティ、の少なくとも１つの選択を受信する動作（act）と、

前記受信した少なくとも１つの通信プロパティ選択がサポートされているか否かを判定

するため、また前記クライアント・コンピュータ・システムがサポートする他の関連通信プロパティを特定するために、前記クライアント・コンピュータ・システムに問い合わせる動作（act）と、

任意の選択された通信プロパティと前記クライアント・コンピュータ・システムがサポートする特定された他の関連通信プロパティとに従って前記クライアント・コンピュータ・システムとのＨＴＴＰ通信を処理するように前記通信フィルタを構成する動作（act）と

を備えることを特徴とする方法。

【請求項３１】

前記ログイン・ページから選択可能な前記１つまたは複数の選択可能な通信プロパティの少なくとも１つの選択を受信する前記動作（act）は、前記クライアント・コンピュータ・システムの信頼性を指示する通信プロパティ選択を受信する動作（act）を備えることを特徴とする請求項３０に記載の方法。

【請求項３２】

前記ログイン・ページから選択可能な前記１つまたは複数の選択可能な通信プロパティの少なくとも１つの選択を受信する前記動作（act）は、前記クライアント・コンピュータ・システムのコンテンツ処理能力および／または所望の機能レベルを指示する通信プロパティ選択を受信する動作（act）を備えることを特徴とする請求項３０に記載の方法。

【請求項３３】

前記クライアント・コンピュータ・システムに問い合わせる前記動作（act）は、前記クライアント・コンピュータ・システムがＨＴＴＰ圧縮をサポートすると決定する動作（act）を備えることを特徴とする請求項３０に記載の方法。

【請求項３４】

クライアント・コンピュータ・システムにおいて、サーバ・コンピュータ・システムに求められる通信プロパティを指示する方法であって、

前記サーバによるＨＴＴＰメッセージの処理方法を変更することができる１つまたは複数の選択可能な通信プロパティを選択するためのインターフェースを含むログイン・ページをサーバ・コンピュータ・システムから受信する動作（act）と、

前記クライアント・コンピュータ・システムで前記ログイン・ページを提示する動作（act）と、

前記ログイン・ページで前記１つまたは複数の通信プロパティの少なくとも１つの選択を受信する動作（act）と、

前記クライアント・コンピュータ・システムとのＨＴＴＰ通信の処理方法を通信フィルタに指示する前記通信プロパティ選択を前記サーバ・コンピュータ・システムの前記通信フィルタに送信する動作（act）と

を備えることを特徴とする方法。

【請求項３５】

前記ログイン・ページで前記１つまたは複数の通信プロパティの少なくとも１つの選択を受信する前記動作は、前記クライアント・コンピュータ・システムの信頼性を示す選択を受信する動作（act）を備えることを特徴とする請求項３４に記載の方法。

【請求項３６】

前記ログイン・ページで前記１つまたは複数の通信プロパティの少なくとも１つの選択を受信する前記動作（act）は、前記クライアント・コンピュータ・システムのコンテンツ処理能力および／または所望の機能レベルを指示する選択を受信する動作（act）を備えることを特徴とする請求項３４に記載の方法。

【請求項３７】

前記通信プロパティ選択を前記サーバ・コンピュータ・システムの通信フィルタに送信する前記動作（act）は、前記通信プロパティ選択をユーザの資格証明書と共に送信する動作（act）を備えることを特徴とする請求項３４に記載の方法。

【請求項３８】

サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを試みるクライアント・コンピュータ・システムで使用するための、前記リソースへのアクセスが許可されるために使用されるクライアント側の資格証明書をセキュリティ保護する方法を実装するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記クライアント・コンピュータ・システムに、

前記リソースへのウェブ・ベースのアクセスを求める第１の要求を送信すること、

ユーザの資格証明書を受け入れるためのインターフェースを提供するログイン・ページにリダイレクトされること、

前記ログイン・ページを使用して、前記サーバ・コンピュータ・システムにユーザの資格証明書を提出すること、

前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵とは両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を受信すること、および

前記リソースへのウェブ・ベースのアクセスを求める、前記暗号化された情報をこの時点で含む、第２の要求を送信すること

を実行させるコンピュータ実行可能命令を記憶している１つまたは複数のコンピュータ可読媒体を備えることを特徴とするコンピュータ・プログラム製品。

【請求項３９】

前記１つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項３８に記載のコンピュータ・プログラム製品。

【請求項４０】

クライアント・コンピュータ・システムから、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を受信するサーバ・コンピュータ・システムで使用するための、前記リソースへのアクセスが許可されるために使用されるべきクライアント側の資格証明書をセキュリティ保護する方法を実施するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記サーバ・コンピュータ・システムに、

前記クライアント・コンピュータ・システムによって送信された、前記リソースへのウェブ・ベースのアクセスを求める第１の要求を受信すること、

前記第１の要求に呼応して、前記クライアント・コンピュータ・システムがユーザの資格証明書を入力することのできるログイン・ページに前記クライアント・コンピュータ・システムをリダイレクトすること、

前記ログイン・ページで提出された前記ユーザの資格証明書を受信すること、

前記提出されたユーザの資格証明書の少なくとも一部と時間依存署名とを表す暗号化された情報であって、前記時間依存署名は前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されている、前記暗号化された情報を送信すること、および

前記リソースへのウェブ・ベースのアクセスを求める、前記クライアント・コンピュータ・システムから送信された、前記暗号化された情報を含む、第２の要求を受信すること

を実行させるコンピュータ実行可能命令を記憶している１つまたは複数のコンピュータ可読媒体を備えるコンピュータ・プログラム製品。

【請求項４１】

前記１つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項４０に記載のコンピュータ・プログラム製品。

【請求項４２】

サーバ・コンピュータ・システムで使用するための、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスのために使用されるユーザの資格証明書の有効

性を決定する方法を実装するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記サーバ・コンピュータ・システムに、
前記サーバ・コンピュータ・システムの前記リソースへのウェブ・ベースへのアクセスを求める、一意のセッションＩＤと、ユーザの資格証明書の少なくとも一部および時間依存署名を表す暗号化された情報とを含む要求であって、前記時間依存署名は、前記ユーザの資格証明書の前記少なくとも一部と署名時間依存鍵とから導出され、前記暗号化された情報は暗号時間依存鍵を使用して暗号化され、前記署名時間依存鍵と前記暗号時間依存鍵は両方とも循環鍵ストアの鍵から引き出されていること、
前記循環鍵ストアの前記最新の鍵を使用して前記ユーザの資格証明書の前記少なくとも一部の有効性確認を試みること、
前記要求されたリソースへのウェブ・ベースのアクセスを制御するモジュールに前記要求を転送すること、および
前記ユーザの資格証明書の前記少なくとも一部と時間依存署名とを表すリフレッシュされた暗号化された情報が前記循環鍵ストアの前記最新の鍵から導出されているか否かを判定すること
を実行させるコンピュータ実行可能命令を記憶している１つまたは複数のコンピュータ可読媒体を備えることを特徴とするコンピュータ・プログラム製品。
【請求項４３】
前記１つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項４２に記載のコンピュータ・プログラム製品。
【請求項４４】
メッセージ・ヘッダーを変更することができる通信フィルタを含むサーバ・コンピュータ・システムで使用するための、クライアント・コンピュータ・システムに関連付けられた通信プロパティを決定する方法を実施するための、コンピュータ・プログラム製品であって、プロセッサによって実行された場合に、前記サーバ・コンピュータ・システムに、
ＨＴＴＰメッセージの処理方法を変更することのできる１つまたは複数の選択可能な通信プロパティを選択するためのインターフェースを含むログイン・ページを前記クライアント・コンピュータ・システムに送信すること、
前記ログイン・ページから選択可能な前記１つまたは複数の選択可能な通信プロパティで、前記クライアント・コンピュータ・システムとのＨＴＴＰ通信の処理方法を前記通信フィルタに示すプロパティ、の少なくとも１つの選択を受信すること、
前記受信した少なくとも１つの通信プロパティ選択がサポートされているか否かを判定するため、また前記クライアント・コンピュータ・システムがサポートする他の関連通信プロパティを特定するために、前記クライアント・コンピュータ・システムに問い合わせること、
任意の選択された通信プロパティと前記クライアント・コンピュータ・システムがサポートする特定された他の関連通信プロパティとに従って前記クライアント・コンピュータ・システムとのＨＴＴＰ通信を処理するように前記通信フィルタを構成すること
を実行させるコンピュータ実行可能命令を記憶している１つまたは複数のコンピュータ可読媒体を備えることを特徴とするコンピュータ・プログラム製品。
【請求項４５】
前記１つまたは複数のコンピュータ可読媒体は、物理媒体であることを特徴とする請求項４４に記載のコンピュータ・プログラム製品。
【請求項４６】
ＨＴＴＰメッセージをフィルタリングするよう構成されたサーバ・コンピュータ・システムであって、
１つまたは複数の処理装置と、
１つまたは複数のコンピュータ可読媒体であって、
ＨＴＴＰメッセージを受信し、
前記ＨＴＴＰメッセージに含まれる一意のセッションＩＤに基づいて前記ＨＴＴＰメッ

セージを送信したクライアント・コンピュータ・システムを特定し、
前記クライアント・コンピュータ・システムに関連付けられたクライアントの状態情報にアクセスし、
ユーザの資格証明書と時間依存署名とを表す暗号化された情報の有効性確認を試み、
前記クライアントの状態情報で示された通信プロパティに基づいて前記ＨＴＴＰメッセージが変更されるべきか否かを判定する
ように構成されている１つまたは複数のコンピュータ可読媒体と
を備えることを特徴とするサーバ・コンピュータ・システム。
【請求項４７】
リソースへのウェブ・ベースのアクセスのための資格証明書情報を安全に表記するためのフォーマットを規定するデータ構造を記憶している１つまたは複数のコンピュータ可読媒体であって、前記データ構造は、
前記リソースへのウェブ・ベースのアクセスを制御するモジュールで認証するためのユーザの資格証明書を表記する資格証明書フィールドと、
前記モジュールと前記資格証明書フィールドに表されている前記ユーザの資格証明書を提出したクライアント・コンピュータ・システムとの間でＨＴＴＰメッセージを転送する場合に使用されるべき１つまたは複数の通信プロパティを表記するフラグ・フィールドと、
前記資格証明書フィールドに表されている前記ユーザの資格証明書と前記フラグ・フィールドに表されている前記通信プロパティとを有効性確認するために使用することができる時間依存デジタル署名を表すハッシュ・メッセージ認証コード・フィールドと
を備えることを特徴とする１つまたは複数のコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータ・ネットワークに関し、より詳細には、リソースに対するウェブ・ベースのアクセスに使用されるクライアントの資格証明書（credentials）を安全に処理することに関する。
【背景技術】
【０００２】
コンピュータ・システムおよび関連技術は、社会の多くの側面に影響を与える。実際、情報を処理するコンピュータ・システムの機能は、我々の生活および仕事の方法に変化を与えてきた。現在、コンピュータ・システムは、一般に、コンピュータ・システムが出現する前には手作業で行われていた多くの作業（例えば、文書処理、スケジューリング、およびデータベース管理）を実行している。さらに最近では、コンピュータ・システムは相互に結合されて、コンピュータ・システムが有線と無線のコンピュータ・ネットワークの両方を構成し、それを介してコンピュータ・システムが電子的に通信し、データを共有することができるようになった。その結果、コンピュータ・システムで実行される多くのタスク（例えば、音声通信、電子メールへのアクセス、電子会議、ウェブ・ブラウジング）には、１つまたは複数の他のコンピュータ・システムとの無線および／または有線コンピュータ・ネットワークを介した電子通信が含まれている。
【０００３】
特に、電子メールは、通信のための重要な方法になった。電子メールのシステムは、通常、電子メール・クライアント装置と電子メール・サーバ装置とを含む。これらの装置は、通常、コンピュータ・システム（例えば、サーバ、ＰＣ、ラップトップ、およびＰＤＡ）上で実行されるように構成されたソフトウェア・アプリケーションである。電子メール・クライアント装置と電子メール・サーバ装置は、通常、相互の特定動作用に設計・構成されている。電子メール・クライアント装置と電子メール・サーバ装置は、一般に、例えばクライアント・コンピュータ・システムのアプリケーション・プログラムがサーバ・コンピュータ・システム上のプログラムを実行することを可能にする、リモート・プロシー

ジャ・コール（「ＲＰＣ：Remote Procedure Calls」）のような独自開発のプロトコルを使用して相互に通信する。例えば、電子メール・クライアント装置は、電子メール・サーバ装置に適切な引数によってメッセージを送信することができ、電子メール・サーバ装置は電子メール・メッセージを返信する。

【０００４】

電子メール・サーバの一部の種類は、専用電子メール・クライアントではなく、例えばウェブ・ブラウザを有するクライアント・コンピュータ・システムのような「ゼロタッチ（zero-touch）」クライアントを介して電子メールにアクセスできるよう構成されている。これらの種類の電子メール・サーバでは、ウェブ・ブラウザは電子メール・サーバと対話し、クライアントシステム上で実行することが必要な機能ならばどのような機能でもウェブ・ブラウザを介して実行される。例えば、クライアント・コンピュータ・システムは、ウェブ・ブラウザが電子メール・サーバと適切に対話することを可能にするハイパー・テキスト・マークアップ言語（「ＨＴＭＬ」）命令とスクリプト（アクティブ・サーバ・ページのような技術によって動的に生成される）をダウンロードすることができる。すなわち、ゼロタッチのブラウザ・ベースのクライアントは、ユーザが、自分の電子メールと、ゼロタッチのブラウザ・ベースのクライアントによって共通ネットワーク（例えば、ワールドワイドウェブ（「ＷＷＷ」））に接続されている任意のサーバ・コンピュータ・システムからの他のメール関連情報（例えば、カレンダーおよび共用フォルダ）とにアクセスすることを可能にする。したがって、例えばＷＷＷ上のウェブ・ベースのコンテンツにアクセスするために使用されるハイパー・テキスト転送プロトコル（「ＨＴＴＰ」）のようなプロトコルを、電子メールおよび他のメール関連情報にアクセスするために使用することもできる。

【０００５】

しかし、電子メールおよび他のメール関連情報へのブラウザ・ベースのアクセス可能性は潜在的なセキュリティ問題をもたらし、いくつかのセキュリティ問題はウェブ・ブラウザ・メモリ内のユーザの資格証明書のキャッシングに関連している。ウェブ環境において、コンテンツおよびコンテンツに対する要求（request）は、一般にＨＴＴＰを使用して配送される。例えば、コンテンツへのアクセスを求めるＨＴＴＰ要求がブラウザ・ベースのクライアントのユーザからネットワークに向けて配送される。次いで要求はサーバ・コンピュータ・システムのウェブ・サーバで受信され、そこでその要求を処理して要求したコンテンツにアクセスすることをブラウザ・ベースのクライアントのユーザが許可されているか否かを判定する。ユーザが要求したコンテンツにアクセスすることを許可されている場合、ウェブ・サーバはコンテンツをＨＴＴＰメッセージでブラウザ・ベースのクライアントに返信する。

【０００６】

ＨＴＴＰの一部のバージョン（例えば、ＨＴＴＰ／１．０）はステートレス（stateless）である。すなわち、ＨＴＴＰを介した通信（例えば、電子メール・メッセージの要求）は、サーバによる以前のいかなる通信に関する知識（例えば、電子メール・メッセージに対する他の以前の要求）なしに実行される。したがって、ＨＴＴＰのこれらのバージョンは、ユーザが「ログイン」または「ログアウト」する「セッション」の概念をサポートしない。ＨＴＴＰの他のバージョン（例えば、ＨＴＴＰ／１．１）は、ＨＴＴＰ接続を存続状態（alive）に保つよう試みるためにクライアントとサーバの間で送信される「キープアライブ（keep-alive）」メッセージをサポートする。しかし、キープアライブ・メッセージの使用は、やや信頼性に乏しく、キープアライブ・メッセージが使用される場合であっても、ＨＴＴＰ接続がアクティブに保たれる保証はない。さらに、クライアントの要求が複数のユーザ間でキープアライブ・リンクを共用する中間プロキシ・サーバを介して頻繁に送り込まれるので、受信した要求が以前に認証されたクライアントによって送信されたか否かをサーバが判定することはない。したがって、ＨＴＴＰ接続がステートレスか、またはキープアライブ・メッセージを使用しているかに関わらず、ＨＴＴＰを介して配送されるコンテンツへのアクセスを求める各要求（以下、「ＨＴＴＰ要求」と呼ぶ）は、

適切なＨＴＴＰ認証情報（authentication information）を含む必要がある。

【０００７】

したがって、ＨＴＴＰ認証情報は、ＷＷＷ－許可（Authorization）ヘッダーと呼ばれ、「ＷＷＷ－許可：［認証－タイプ］［資格証明書（Credentials）］」というフォーマットを有する特別なヘッダーを介してＨＴＴＰ要求に含めることができる。ウェブ・ブラウザが最初に認証を必要とするコンテンツ（例えば、ユーザが入力した資格証明書の提出）へのアクセスを試みると、ウェブ・サーバは、通常、要求されたコンテンツを提供することを拒否し、代わりにステータス・コード４０１「無許可（Unauthorized）」を有するＨＴＴＰメッセージを返信する。このＨＴＴＰ応答（responce）メッセージには、「ＷＷＷ－認証（Authenticate）：［認証方法］［領域＝領域値］［任意選択情報］」というフォーマットのヘッダーが含まれる。

【０００８】

ウェブ・ブラウザで返信を受信すると、ＨＴＴＰ応答メッセージは、ウェブ・ブラウザに、例えばユーザ名およびパスワードのような資格証明書を要求するダイヤログボックスを提示させる。ユーザが資格証明書を入力した後、ウェブ・ブラウザは、元のＨＴＴＰ要求を、入力された資格証明書を含むＨＴＴＰ　ＷＷＷ－認証ヘッダーと共に再送する。ウェブ・サーバが、ユーザの入力した資格証明書を有効であるとして受け入れて、要求されたコンテンツ（例えば、電子メール・メッセージ）を返信した場合、ウェブ・ブラウザは、ユーザが入力した資格証明書をブラウザのメモリにキャッシュする。したがって、同じユニフォーム・リソース・ロケータ（「ＵＲＬ」）または同じコンテンツに関連付けられた対応する派生的な関連ＵＲＬへのそれ以降の要求では、キャッシュされた資格証明書がブラウザのメモリから取り出され、対応するＨＴＴＰ　ＷＷＷ－許可ヘッダーに含められる。この結果、ＨＴＴＰがステートレスであっても、ユーザは、同じまたは対応する派生的な関連ＵＲＬに対するそれぞれの要求について資格証明書を再入力する必要から、開放される。

【発明の開示】

【発明が解決しようとする課題】

【０００９】

残念ながら、ウェブ・ブラウザは、一般に、（ウェブブラウザプログラムを終了する（quitting）か、またはコンピュータ・システムまたはクライアントのデバイスを再起動（re-booting）またはターン・オフすることによって）ウェブ・ブラウザが終了されるまで、キャッシュされた資格証明書を基本的に無期限でブラウザのメモリに保持する。したがって、保護されたコンテンツにアクセスした特権のあるユーザの資格証明書は、そのユーザがそのウェブ・ブラウザを使用しなくなった後でもブラウザのメモリにキャッシュされている可能性がある。次いで特権のあるユーザがコンピュータ・システムのそばを離れた場合、別の特権のないユーザがやってきて、ブラウザの戻りボタンまたは履歴機能を使用して保護されたコンテンツへのアクセスを試みる可能性がある。特権のあるユーザの資格証明書がブラウザのメモリに依然としてキャッシュされているので、ウェブ・ブラウザは、キャッシュされた資格証明書を取り出し、それらを保護されたコンテンツにアクセスする特権のないユーザの要求と共に提出する。したがって、特権のないユーザが、ウェブ・ブラウザで適切な資格証明書を入力することを必要とせずに、保護されたコンテンツへのアクセスを得る可能性がある。

【００１０】

キャッシュされた資格証明書は、ウェブ・ブラウザを終了することを許可しない公共のコンピュータおよび／またはコンピュータ・システムのある場所では特に問題となり得る。そのようなコンピュータ・システムの一例としてインターネット・キオスクがある。インターネット・キオスクは、一般大衆にインターネットへのアクセスを提供するために、例えば図書館、インターネットカフェ、および会議センターのような公共の場所に置かれることがしばしばある。インターネット・キオスクは、キオスクのある場所に来た人なら誰でも、最初にウェブ・ブラウザを探して起動することを必要とせずに迅速にインターネ

ットにアクセスすることを可能にするよう設計されている。したがって、多くのインターネット・キオスクは、ウェブ・ブラウザが常時活動状態にあり終了されることがないように構成されている。

【００１１】

この結果、インターネットへの効率的なアクセスが提供されるが、またキャッシュされた資格証明書が基本的に無期限でブラウザのメモリに残存することにもなる。例えば特権のあるユーザが（例えば、保護されたコンテンツにアクセスするために）インターネット・キオスクに資格証明書を入力する場合、その特権のあるユーザの資格証明書はブラウザのメモリにキャッシュされる。ウェブ・ブラウザは終了されるはずがないので、その公共のキオスクの電源を切らずにキャッシュされた資格証明書を除去する方法は基本的にない。したがって、特権のあるユーザがキャッシュされた資格証明書を消す方法を知っていたとしても（例えば、ウェブ・ブラウザを終了することによって）、特権のあるユーザがそれを実行することから、防止されているかもしれない。

【００１２】

保護されたコンテンツにアクセスするためにキャッシュされた資格証明書を使用することは、ブラウザ・ベースの電子メールアプリケーションにとって特別重要な問題である。例えば、特権のないユーザは、ページを戻して個人的なデータを含んでいる可能性のある特権のあるユーザの電子メール・メッセージにアクセスすることができる。特権のあるユーザの電子メールにアクセスすることに加え、キャッシュされた資格証明書は特権のないユーザが特権のあるユーザになりすますことを可能にする場合もある。例えば、特権のないユーザは、特権のあるユーザに関連付けられたアカウントから電子メール・メッセージを送信することができる場合がある。

【００１３】

この問題に対する１つの可能な解決法は、コンテンツが要求されるたびにユーザに再認証を強制することである。しかしこれにより、ユーザはコンテンツにアクセスするＨＴＴＰ要求ごとに認証情報を手動で再入力することが要求される。ウェブ・サイトとの通常の対話は数十または場合によっては数百のＨＴＴＰ要求から構成される場合があるので、ユーザは数十回、または数百回も資格証明書を再入力しなければならないことになる。したがって、ＨＴＴＰ要求ごとに資格証明書を再入力することは、コンテンツにアクセスするために必要な時間とデータ入力の量を大幅に増加させることになる。この解決法は多くのユーザにとってあまりにも煩雑すぎ、ユーザは、１回のセッションに自分の資格証明書を１回だけ入力することを好む。したがって、ウェブ・ベースのリソースへのアクセスに使用されるクライアントの資格証明書を安全に処理するシステム、方法、コンピュータ・プログラム製品が有利になるであろう。

【課題を解決するための手段】

【００１４】

従来技術における前述の問題は、本発明の原理によって解決され、本発明の原理は、リソースへのウェブ・ベースのアクセスのために使用されるクライアントの資格証明書を安全に処理する方法、システム、コンピュータ・プログラム製品、およびデータ構造に向けられている。クライアント・コンピュータ・システム（以下、「クライアント」と呼ぶ）と、サーバ・コンピュータ・システム（以下、「サーバ」と呼ぶ）は、例えばインターネットのような共通のネットワークに接続されている。サーバは、例えば電子メール・メッセージおよび関連するメール・データのようなリソースへのウェブ・ベースのアクセスを可能にするように構成されている。クライアントは、ウェブ・ベースのリソースへのアクセスを要求し、ウェブ・ベースのリソースをそのクライアントのユーザに提示することのできる、ブラウザを含んで構成されている。

【００１５】

クライアントは、サーバのリソースにアクセスすることを求める第１の要求を送信する。例えば、クライアントは、サーバに記憶されている電子メール・メッセージへのアクセスを求める要求を送信することができる。サーバは第１の要求を受信するが、クライアン

トが無許可であるため、サーバは第１の要求の受信に呼応してそのクライアントをログイン・ページにリダイレクトする。クライアントをリダイレクトすることは、サーバがクライアントに、ログイン・ページへのユニフォーム・リソースＩＤ（Identifier）（「ＵＲＩ」）と共にリダイレクション・インジケータ（例えば、ステータス・コード３０２「一時移動」を有するハイパー・テキスト転送プロトコル（「ＨＴＴＰ」）メッセージ）を含む応答を送信することを含むことができる。このログイン・ページは、クライアントのユーザがユーザの資格証明書を入力するためのインターフェースを提供するアクティブ・サーバ・ページ（「ＡＳＰ」）ページであってよい。クライアントはこのログイン・ページにアクセスし、そのログイン・ページを使用してユーザの資格証明書をサーバに提出する。クライアントは、例えばＨＴＴＰポストをセキュリティ保護するためにセキュア・ソケット・レイヤ（「ＳＳＬ」）を使用して、資格証明書を提出することができる。

【００１６】

サーバは提出された資格証明書を受信する。サーバは、ユーザの資格証明書と時間依存デジタル署名を表す暗号化された情報を送信する。サーバは、認証を実行する信頼された機関に、提出された資格証明書についての認証を委任した後、暗号化された情報を送信する場合がある。サーバは、循環鍵ストア（rotating key store）の鍵を使用して暗号化されたデータを生成する。循環鍵ストアの各鍵は指定時間間隔（例えば１０分）後に自動的に期限が切れる。指定時間間隔後、サーバは循環鍵ストア内に新しい鍵を循環させ、期限切れの鍵を循環鍵ストアから取り外すように循環させることができる。循環鍵ストアで保持される鍵の数と指定時間間隔は管理者が構成することができる。

【００１７】

ユーザの資格証明書が受信されると、サーバはユーザの資格証明書を一意識別子（例えば、グローバル一意識別子（「ＧＵＩＤ」））に関連付ける。サーバは、循環鍵ストアの最新の鍵と一意識別子と第１の定数列との組み合わせを（例えば、ＳＨＡ－１またはＭＤ－５ハッシング・アルゴリズムを使用して）ハッシュすることによって、データにデジタル的に署名するために使用することができる、署名鍵を導出する。次いでサーバは、この署名鍵を使用して、一意識別子とユーザの資格証明書の組み合わせからデジタル署名（例えば、ハッシュ・メッセージ認証コード（「ＨＭＡＣ」））を導出する。

【００１８】

サーバは、データを暗号化するために使用することのできる暗号鍵も、循環鍵ストアの最新の鍵と一意識別子と第２の定数列との組み合わせをハッシュすることによって、導出する。次いでサーバは、この暗号鍵を使用して、デジタル署名とユーザの資格証明書の組み合わせを、暗号化された情報の中に暗号化する。サーバは、一意識別子と暗号化された情報とをクライアントに送信する。クライアントは、この一意識別子と暗号化された情報を受信し、一意識別子と暗号化された情報を（例えば対応するクッキーに）格納する。

【００１９】

クライアントは、サーバのリソースへのアクセスを求める、一意識別子と暗号化された情報を含む第２の要求を送信する。サーバは、第２の要求を受信し、循環鍵ストア中の最新の鍵を使用してユーザの資格証明書の有効性確認を試みる。サーバは、循環鍵ストアの最新の鍵と一意識別子と第２の定数列との組み合わせをハッシュすることによって、データを暗号解読するために使用することのできる、暗号解読鍵を導出する。サーバは、暗号解読鍵を使用して暗号化された情報を暗号解読し、それによってデジタル署名とユーザの資格証明書を明らかにする（平文にする）。サーバは、循環鍵ストアの最新の鍵と一意識別子と第１の定数列との組み合わせとをハッシュすることによって、データを認証するために使用することのできる、有効性確認鍵を導出する。サーバは、有効性確認署名鍵を使用して、一意識別子とユーザの資格証明書の組み合わせから有効性確認デジタル署名を導出する。

【００２０】

サーバは、有効性確認デジタル署名をデジタル署名と比較する。有効性確認デジタル署名とデジタル署名が一致した場合、ユーザの資格証明書は有効であるとされる。一方、有

効性確認デジタル署名とデジタル署名が一致しない場合、資格証明書は有効であるとされない。ユーザの資格証明書が、循環鍵ストアの最新の鍵を使用して有効であるとされない場合、循環鍵ストア内で次の最も新しい鍵が使用され（例えば、次の最も新しい鍵を使用して暗号解読鍵と有効性確認デジタル署名を生成することにより）、ユーザの資格証明書の有効性確認が試みられる。サーバは、循環鍵ストアの各鍵を使用してユーザの資格証明書の有効性確認を試みることができる。有効であるとされたユーザの資格証明書は、要求されたリソース（例えば、電子メール・メッセージ）へのアクセスを制御するモジュール（例えば、電子メール・サーバ）に転送される。

【００２１】

ユーザの資格証明書が、循環鍵ストアの最新の鍵ではない鍵によって有効であるとされた場合、サーバはリフレッシュされた暗号化された情報を導出すべきであると判定する。サーバは、循環鍵ストアの最新の鍵を使用して、（例えば、リフレッシュされたデジタル署名とリフレッシュされた暗号鍵を最新の鍵から導出することにより）リフレッシュされた暗号化された情報を導出する。有効であるとされたユーザの資格証明書が適切である場合、要求されたリソースが、リフレッシュされた暗号化された情報を適宜ともなってクライアントに返信される。クライアントは、リソースと任意のリフレッシュされた暗号化された情報を受信する。クライアントは、任意のリフレッシュされた暗号化された情報で一意識別子に対応する以前に暗号化された情報を上書きして記憶する。ユーザの資格証明書が循環鍵ストアのいかなる循環鍵を使用しても有効であるとすることができない場合、クライアントは、新しいユーザの資格証明書を入力することができるログイン・ページにリダイレクトされる。

【００２２】

いくつかの実施形態では、ログイン・ページはＨＴＴＰメッセージの処理方法を変更することができる通信プロパティ（例えば、ｇｚｉｐ圧縮に対するサポートについて、クライアント・コンピュータ・システムがプライベートであるかまたは信頼性のないクライアントであるかについて、クライアントが簡素化したコンテンツを好む上級のクライアントであることについてのプロパティ）を選択するためのインターフェースを含む。通信プロパティはログイン・ページで選択され、クライアントとのＨＴＴＰ通信の処理方法を通信フィルタに示すために通信フィルタに送信される。選択された通信プロパティがサーバで受信される。

【００２３】

サーバは、選択された通信プロパティをクライアントがサポートしているか否かを判定するため、また他の関連通信プロパティを特定するため、クライアントに問い合わせる。サーバは、任意の選択された通信プロパティとクライアントがサポートすると特定された他の関連通信プロパティに従ってクライアントとのＨＴＴＰ通信を処理するよう通信フィルタを構成する。クライアントが安全でない場所にいるということに基づいて、サーバは、循環間隔が短く、より少数の鍵を保持する別の循環鍵ストアを使用することができる。

【００２４】

本発明のさらなる機能および利点は、以下の説明で述べることとし、また一部は以下の説明から明らかになろうし、あるいは本発明を実践することによって知ることができよう。本発明の機能および利点は、特に特許請求の範囲で指摘された機器および組み合わせを使用して実現し、得ることができる。本発明のこれらおよび他の機能は、以下の説明および特許請求の範囲からより完全に明らかになろうし、また以下で述べるように本発明を実践することによって知ることができよう。

【発明を実施するための最良の形態】

【００２５】

本発明の上記および他の利点および機能を得ることができる方法を説明するために、上記で概説した本発明のより具体的な説明が、添付の図面に示す本発明の具体的な実施形態を参照することによって提供される。これらの図面は本発明の典型的な実施形態だけを示しており、したがって本発明の範囲を限定するものとみなされるべきではないということ

を理解して、本発明は、添付の図面を使用してさらなる特殊性および詳細を以って記載し説明される。

【００２６】

本発明の原理は、リソースに対するウェブ・ベースのアクセスのために使用されるクライアントの資格証明書の安全な処理を提供する。サーバは、１つまたは複数の鍵のうち少なくとも１つの循環鍵ストアを保持する。循環鍵ストア中の各鍵は指定時間間隔（例えば１０分）後に自動的に有効期限が切れる。指定時間間隔後、サーバは循環鍵ストア内部に循環新しい鍵を循環させ、循環期限切れの鍵を循環鍵ストアから取り外すように循環させる。循環鍵ストアで保持される鍵の数と指定時間間隔は管理者が構成することができる（例えば、３つの鍵を保持して５分ごとに鍵を循環する）。サーバは、ユーザの資格証明書に対するデジタル署名を生成し、循環鍵ストアの鍵に基づいてユーザの資格証明書を暗号化することによってユーザの資格証明書をセキュリティ保護する。

【００２７】

ユーザの資格証明書を入力するためのインターフェースを有するログイン・ページがクライアントで提示される。クライアントで入力されたユーザの資格証明書はサーバに送信される。ユーザの資格証明書の受信に呼応して、サーバはクライアントに対する一意のセッションＩＤを生成する。サーバは、循環鍵ストアの最新の鍵と一意のセッションＩＤに基づいてユーザの資格証明書に対するデジタル署名を導出する。次いでサーバは、循環鍵ストアの最新の鍵と一意のセッションＩＤから導出した暗号鍵に基づいてデジタル署名とユーザの資格証明書を暗号化する。暗号化された資格証明書がクライアントに返信されると、循環鍵ストアからの鍵が使用されて、資格証明書の有効性確認を試みられる。ユーザの資格証明書を暗号化するために元々使用された循環鍵ストアからの鍵が、循環鍵ストアから取り外すように循環すると、クライアントは、新しい資格証明書を入力するためのログイン・ページにリダイレクトされる。

【００２８】

本発明の範囲にある実施形態は、コンピュータ実行可能命令を搬送し、またはデータ構造を格納するためのコンピュータ可読媒体を含む。このようなコンピュータ可読媒体は、汎用または専用コンピュータ・システムによってアクセス可能な任意の入手可能な媒体であってよい。限定ではなく一例として、このようなコンピュータ可読媒体は、ＲＡＭ、ＲＯＭ、ＥＰＲＯＭ、ＣＤ－ＲＯＭまたは他の光ディスク・ストレージ、磁気ディスク・ストレージまたは他の磁気記憶装置、または所望のプログラム・コード手段をコンピュータ実行可能命令、コンピュータ可読命令、またはデータ構造の形式で搬送または記憶するために使用することができ、汎用または専用コンピュータ・システムによってアクセスすることができるいかなる他の媒体でも含むことができる。

【００２９】

本明細書および特許請求の範囲では、「ネットワーク」をコンピュータ・システムおよび／またはモジュール間で電子データの転送を可能にする１つまたは複数のデータリンクと定義する。情報がネットワークまたは他の通信接続（ハード・ワイヤード、無線、またはハード・ワイヤードと無線の組み合わせのどれか）を介してコンピュータ・システムに送信すなわち提供される場合、接続はコンピュータ可読媒体と厳密にみなされる。したがって、このような接続はどれでも厳密にはコンピュータ可読媒体と呼ばれる。上記の組み合わせもコンピュータ可読媒体の範囲に含まれるべきである。コンピュータ実行可能命令は、例えば汎用コンピュータ・システムまたは専用コンピュータ・システムに特定の関数または一群の関数を実行させる命令およびデータを含んでいる。コンピュータ実行可能命令は、例えばバイナリ、アセンブリ言語のような中間形式の命令、または場合によってはソース・コードであってよい。

【００３０】

本明細書および首記の特許請求の範囲では、「コンピュータ・システム」を、協同して電子データに対していくつかの動作を実行する１つまたは複数のソフトウェア・モジュール、１つまたは複数のハードウェア・モジュール、またはこれらの組み合わせと定義する

。例えばコンピュータ・システムの定義は、パーソナル・コンピュータのハードウェア構成要素、並びにパーソナル・コンピュータのオペレーティング・システムのようなソフトウェア・モジュールを含む。モジュールの物理的レイアウトは重要ではない。コンピュータ・システムは、ネットワークを介して結合された１つまたは複数のコンピュータを含むことができる。同様に、コンピュータ・システムは、（メモリおよびプロセッサのような）内部モジュールが協同して電子データに対していくつかの動作を実行する（携帯電話またはパーソナル・デジタル・アシスタント「ＰＤＡ」のような）単一の物理デバイスを含むことができる。

【００３１】

当業者には、本発明が、パーソナル・コンピュータ、ラップトップ・コンピュータ、ハンドヘルド装置、マルチ・プロセッサ・システム、マイクロプロセッサ・ベースの、すなわちプログラム可能な家庭用電化製品、ネットワークＰＣ、ミニ・コンピュータ、メインフレーム・コンピュータ、携帯電話、ＰＤＡ、ページャなどを含めて多くのタイプのコンピュータ・システム構成を有するネットワーク・コンピューティング環境で実施することができるということが理解されよう。本発明は、（ハード・ワイヤード・データリンク、無線データリンク、またはハード・ワイヤード・データリンクと無線データリンクの組み合わせのどれかによって）ネットワークを介してリンクされたローカル・コンピュータ・システムと遠隔コンピュータ・システムがどちらもタスクを実行する分散型システム環境で実施することもできる。分散型システム環境では、プログラム・モジュールはローカル・メモリ・ストレージ・デバイスと遠隔メモリ・ストレージ・デバイスの両方に置くことができる。

【００３２】

図１および以下の説明は、本発明を実装することができる適切なコンピューティング環境の簡単で一般的な説明を提供することを意図している。必ずしもこの通りである必要はないが、本発明は、コンピュータ・システムが実行しているプログラム・モジュールのようなコンピュータ実行可能命令という一般的な状況で説明する。一般に、プログラム・モジュールは、特定のタスクを実行し、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、構成要素、データ構造などを含む。データ構造に関連付けられたコンピュータ実行可能命令とプログラム・モジュールとは、本明細書で開示された方法の動作を実行するためのプログラム・コード手段の例を表している。

【００３３】

図１を参照すると、本発明を実装するシステム例は、汎用コンピューティング・デバイスを、処理装置１２１とシステム・メモリ１２２と、システム・メモリ１２２を含む様々なシステム構成要素を処理装置１２１に結合するシステム・バス１２３とを含めてコンピュータ・システム１２０の形式で含む。処理装置１２１は、本発明の機能を含めてコンピュータ・システム１２０の機能を実装するように設計されたコンピュータ実行可能命令を実行することができる。システム・バス１２３は、メモリ・バスまたはメモリ・コントローラ、周辺バス、および様々なバス・アーキテクチャのどれかを使用するローカルバスを含めたいくつかのタイプのバス構造のどれであってもよい。システム・メモリは、読取専用メモリ（「ＲＯＭ」）１２４とランダム・アクセス・メモリ（「ＲＡＭ」）１２５を含む。起動時などにコンピュータ・システム１２０内の素子間で情報を転送することに役立つ基本ルーチンを含んでいる基本入出力システム（「ＢＩＯＳ」）１２６をＲＯＭ１２４に記憶することができる。

【００３４】

コンピュータ・システム１２０は、磁気ハードディスク１３９から読み取る／に書き込むための磁気ハードディスク・ドライブ１２７、取り外し可能な磁気ディスク１２９から読み取る／に書き込むための磁気ディスク・ドライブ１２８、ＣＤ－ＲＯＭまたは他の光媒体のような取り外し可能な光ディスク１３１から読み取る／に書き込むための光ディスク・ドライブ１３０も含むことができる。磁気ハードディスク・ドライブ１２７、磁気ディスク・ドライブ１２８、および光ディスク・ドライブ１３０は、それぞれにハードディ

スク・インターフェース１３２、磁気ディスクドライブ・インターフェース１３３、および光ドライブ・インターフェース１３４によってシステム・バス１２３に接続される。これらドライブおよびこれらの関連するコンピュータ可読媒体は、コンピュータ・システム１２０に対してコンピュータ実行可能命令、データ構造、プログラム・モジュール、および他のデータの不揮発性ストレージを提供する。本明細書で説明される実施形態は磁気ハードディスク１３９、取り外し可能な磁気ディスク１２９、および取り外し可能な光ディスク１３１を使用しているが、磁気カセット、フラッシュ・メモリ・カード、デジタル多用途ディスク、ベルヌーイ・カートリッジ、ＲＡＭ、ＲＯＭなどを含めてデータを記憶するための他のタイプのコンピュータ可読媒体を使用することもできる。

【００３５】

１つまたは複数のプログラム・モジュールを含んでいるプログラム・コード手段は、オペレーティング・システム１３５、１つまたは複数のアプリケーション・プログラム１３６、他のプログラム・モジュール１３７、およびプログラム・データ１３８を含めて、ハードディスク１３９、磁気ディスク１２９、光ディスク１３１、ＲＯＭ１２４、またはＲＡＭ１２５に記憶することができる。ユーザは、キーボード１４０、ポインティング・デバイス１４２、または例えばマイクロフォン、ジョイスティック、ゲームパッド、スキャナーなどのような他の入力装置（図示せず）を介してコンピュータ・システム１２０にコマンドおよび情報を入力することができる。これらおよび他の入力装置は、システム・バス１２３に結合されている入出力インターフェース１４６を介して処理装置１２１に接続することができる。入出力インターフェース１４６は、例えばシリアル・ポート・インターフェース、ＰＳ／２インターフェース、パラレル・ポート・インターフェース、ユニバーサル・シリアル・バス（「ＵＳＢ」）インターフェース、または米国電気電子学会（「ＩＥＥＥ」）１３９４インターフェース（すなわち、ＦｉｒｅＷｉｒｅインターフェース）のような幅広い様々な異なるインターフェースのどれでも論理的に表し、または異なるインターフェースの組み合わせを論理的に表すことさえできる。

【００３６】

モニタ１４７または他の表示装置もビデオ・アダプタ１４８を介してシステム・バス１２３に接続される。スピーカー１６９または他の音声出力装置も、音声インターフェース１４９を介してシステム・バス１２３に接続される。例えばプリンターのような他の周辺装置（図示せず）も、コンピュータ・システム１２０に接続することができる。コンピュータ・システム１２０は、例えば事務所全体または企業全体のコンピュータ・ネットワーク、ホームネットワーク、イントラネット、および／またはインターネットのようなネットワークに接続可能である。コンピュータ・システム１２０は、例えば遠隔コンピュータ・システム、遠隔アプリケーション、および／または遠隔データベースのような外部ソースとそのようなネットワークを介してデータを交換することができる。

【００３７】

コンピュータ・システム１２０は、それを介して外部ソースからデータを受信し、かつ／または外部ソースにデータを送信するネットワーク・インターフェース１５３を含む。図１に示すように、ネットワーク・インターフェース１５３は、リンク１５３を介した遠隔コンピュータ・システム１８３とのデータの交換に役立つ。ネットワーク・インターフェース１５３は、ネットワーク・インターフェース・カードおよび対応するネットワーク・ドライバ・インターフェース規約（「ＮＤＩＳ」）スタックのような１つまたは複数のソフトウェアおよび／またはハードウェア・モジュールを論理的に表すことができる。リンク１５１はネットワークの一部（例えば、イーサネット（登録商標）のセグメント）を表し、遠隔コンピュータ・システム１８３はネットワークのノードを表す。例えば遠隔コンピュータ・システム１８３は、コンピュータ・システム１２０にリソース（例えば、電子メール・メッセージ）へのウェブ・ベースのアクセスを提供するサーバ・コンピュータ・システムであってよい。一方、遠隔コンピュータ・システム１８３は、コンピュータ・システム１２０からリソースにアクセスするためにウェブ・ベースのアクセスを使用するクライアント・コンピュータ・システムであってよい。

【００３８】
同様に、コンピュータ・システム１２０は、コンピュータ・システム１２０自体が外部ソースからデータを受信し、かつ／または外部ソースにデータを送信する入出力インターフェース１４６を含む。入出力インターフェース１４６は、コンピュータ・システム１２０がそれを介して外部ソースからデータを受信し、かつ／または外部ソースにデータを送信するリンク１５９を介してモデム１５４（例えば、標準モデム、ケーブルモデム、またはデジタル加入者回線（「ＤＳＬ」）モデム）に結合されている。図１に示すように、入出力インターフェース１４６とモデム１５４は、リンク１５２を介した遠隔コンピュータ・システム１９３とのデータの交換に役立つ。リンク１５２はネットワークの一部を表し、遠隔コンピュータ・システム１９３はネットワークのノードを表す。例えば遠隔コンピュータ・システム１９３は、コンピュータ・システム１２０にリソース（例えば、電子メール・メッセージ）へのウェブ・ベースのアクセスを提供するサーバ・コンピュータ・システムであってよい。一方、遠隔コンピュータ・システム１９３は、コンピュータ・システム１２０からリソースにアクセスするためにウェブ・ベースのアクセスを使用するクライアント・コンピュータ・システムであってよい。

【００３９】
図１は本発明に適したオペレーティング環境を表しているが、本発明の原理は、必要に応じて適切な修正を行い本発明の原理を実装することができるどのシステムでも使用することができる。図１に示した実施形態は説明のみを目的としており、本発明の原理を実装することができる幅広い様々な環境のほんの一部さえも表すものではない。

【００４０】
本発明のモジュール並びに関連するプログラム・データは、コンピュータ・システム１２０に関連付けられたコンピュータ可読媒体のどれからでも記憶し、アクセスすることができる。例えばそのようなモジュールの一部および関連するプログラム・データの一部は、システム・メモリ１２２での記憶用に、オペレーティング・システム１３５、アプリケーション・プログラム１３６、プログラム・モジュール１３７、および／またはプログラム・データ１３８に含めることができる。例えば磁気ハードディスク１３９のような大容量記憶装置がコンピュータ・システム１２０に結合されている場合、そのようなモジュールおよび関連するプログラム・データも大容量記憶装置に記憶することができる。ネットワーク接続された環境で、コンピュータ・システム１２０に関連して示されたプログラム・モジュールまたはその一部は、遠隔コンピュータ・システム１８３および／または遠隔コンピュータ・システム１９３に関連付けられたシステム・メモリおよび／または大容量記憶装置のような遠隔メモリ・ストレージ・デバイスに記憶することができる。そのようなモジュールの実行は、前述のような分散環境で実行することができる。

【００４１】
図２Ａおよび図２Ｂは、クライアントがサーバのリソースへのアクセスを要求する際にクライアント側の資格証明書をセキュリティ保護することに役立つネットワーク・アーキテクチャ２００の一例を示している。クライアント・コンピュータ・システム２０１とサーバ・コンピュータ・システム２１１は、例えばローカル・エリア・ネットワーク（「ＬＡＮ」）、ワイドエリアネットワーク（「ＷＡＮ」）、または場合によってはインターネットのような共通ネットワークに接続することができる。クライアント・コンピュータ・システム２０１は、リソースへのウェブ・ベースのアクセスを要求し、受信したリソースをクライアント・コンピュータ・システム２０１で提示するために使用することのできるブラウザ２０２を含む。クッキー２０３は、サーバ・コンピュータ・システムから以前に受信したデータの一部を記憶する１つまたは複数のクッキーを含むことができる。クッキー２０３内のデータは、個人的な情報または好みをサーバ・コンピュータ・システムに示し、かつ／または記憶されている情報の一部を手動で入力するユーザの手間を省くために、対応するサーバ・コンピュータ・システムに送信されることがある。

【００４２】
サーバ・コンピュータ・システム２１１は、例えば電子メール・メッセージ、アドレス

ブック情報、およびカンレンダリング情報のような電子メール・リソースへのアクセスを提供する電子メール・サーバ２１２を含む。電子メール・リソースにアクセスする許可を得るには、ユーザは電子メール・サーバ２１２によって認証するために電子メール・サーバ２１２に資格証明書を提供することが要求される場合がある。電子メール・サーバ２１２は、電子メール・リソースへのアクセスを求める要求が承諾されるべきか否かを判定するために、受信した資格証明書を資格証明書データベース２１３の許可された資格証明書と比較することができる。ユーザが許可されている場合、電子メール・サーバ２１２は、要求された電子メール・リソースを要求側のクライアント・コンピュータ・システムに返信することができる。ユーザが許可されていない場合、電子メール・サーバ２１２は、無許可メッセージ（例えば、ステータス・コード４０１「無許可」を有するハイパー・テキスト転送プロトコル（「ＨＴＴＰ」）メッセージ）を要求側クライアント・コンピュータ・システムに返信することができる。

【００４３】

サーバ・コンピュータ・システム２１１は、鍵（キー）生成モジュール２１４も含むことができる。鍵生成モジュール２１４は、循環鍵（キー）群２２０に新しい鍵を生成して循環させることができ、期限切れの鍵を循環鍵群２２０から取り外すように循環させることができる。鍵生成モジュール２１４は、１つまたは複数の循環鍵ストアを保持するように構成することができる。例えばネットワーク・アーキテクチャ２００で、鍵生成モジュール２１４は、非信頼用の循環鍵（キー）ストア２２１とプライベート循環鍵（キー）ストア２３１を保持する。

【００４４】

鍵が循環される際の指定時間間隔は設定可能である。すなわち、指定された間隔で循環鍵ストア内に新たに生成された鍵を循環させ、期限切れになった鍵を循環鍵ストアから除去するよう鍵生成モジュール２１４を構成することができる。例えば、鍵生成モジュール１２４は、１０分ごとに、新しい鍵をプライベート循環鍵ストア２３１に挿入し、期限切れの鍵をプライベート循環鍵ストア２３１から除去することができる。循環鍵ストアで保持されている鍵の数も構成可能である。すなわち鍵（キー）生成モジュール２１４は、循環鍵ストア内に指定された数の鍵を保持するように構成することもできる。例えば、鍵生成モジュール２１４は、非信頼用の循環鍵ストア２２１内に３つの鍵を保持するように構成することができる。

【００４５】

保持される鍵の数と指定された間隔は循環鍵ストアによって異なる場合がある。例えば、鍵生成モジュール２１４は、非信頼用の鍵ストア２２１内に５分という指定された循環間隔で３つの鍵を保持し、プライベート鍵ストア２３１内に１時間という指定された循環間隔で４つの鍵を保持することができる。クライアント・コンピュータ・システムに関連付けられたプロパティに応じて、本発明の原理を実装するために異なる鍵ストアを使用することができる。循環鍵ストアの鍵の下に示した矢印は、循環鍵ストアが循環して最終的に期限切れの鍵が出るまで、新しい鍵が追加されるとこれらの鍵が循環に従って送られていくことを示している。例えば、プライベート循環鍵ストア２３１に新しい鍵が追加されると、鍵２３２は循環に従って鍵２３３の位置に入る。

【００４６】

サーバ・コンピュータ・システム２１１はログイン・ページ２１７も含む。ログイン・ページ２１７は、ユーザの資格証明書を提出し、クライアント・コンピュータ・システムに関連付けられた通信プロパティを選択するためのインターフェースを提供するウェブ・ページ（例えば、アクティブ・サーバ・ページ「ＡＳＰ」ページ）であってよい。クライアント・コンピュータ・システムがログイン・ページ２１７に対応するユニフォーム・リソースＩＤ（「ＵＲＩ」）にアクセスすることに呼応して、サーバ・コンピュータ・システム２１１はログイン・ページ２１７をクライアント・コンピュータ・システムに送信することができる。クライアント側のブラウザはクライアント・コンピュータ・システムでログイン・ページ２１７を提示することができる。ログイン・ページ２１７で提出された

ユーザの資格証明書と通信プロパティの選択は、サーバ・コンピュータ・システム２１１に送信することができる。

【００４７】

サーバ・コンピュータ・システムは通信フィルタ２４３も含む。通信フィルタ２４３は、例えばサーバ・コンピュータ・システム２１１の中へ／から外へ送信される要求、応答、およびメッセージのようなＨＴＴＰ通信をインターセプト（intercept）することができる。通信フィルタ２４３は、暗号化されたクッキーに含まれるクライアント状態情報を参照して、サーバ・コンピュータ・システム２１１とクライアント・コンピュータ・システムの間のＨＴＴＰ通信を（例えば、ＨＴＴＰヘッダーを修正することによって）変更すべきか否かを判定すすることができる。通信フィルタ２４３は、循環鍵ストアの鍵を使用して）暗号アルゴリズムを実装して、ユーザの資格証明書を暗号解読し有効性確認することもできる。

【００４８】

サーバ・コンピュータ・システム２１１は、ログイン要素バリデータ（validator；検証器）２１６も含む。ログイン要素バリデータ２１６は、ログイン・ページ２１７で入力されて提出されたユーザの資格証明書を受信することができ、（循環鍵ストアの鍵を使用して）暗号アルゴリズムを実装して、提出されたユーザの資格証明書をデジタル署名し、暗号化することができる。ログイン要素バリデータ２１６は、サーバ・コンピュータ・システム２１１のリソースへのウェブ・ベースのアクセスを要求するクライアント・コンピュータ・システムのために、一意のセッションＩＤ（例えば、グローバル一意識別子（「ＧＵＩＤ」））を生成することもできる。ログイン要素バリデータ２１６は、一意のセッションＩＤと、ユーザの資格証明書および時間依存デジタル署名を含む暗号化された情報とをクライアント・コンピュータ・システムに送信することができる。例えば、ログイン要素バリデータ２１６は、一意のセッションＩＤと暗号化されたユーザの資格証明書を、クッキー２０３での記憶用にクライアント・コンピュータ・システム２０１に送信することができる。

【００４９】

図３は、クライアントがサーバのリソースへのアクセスを要求する際にクライアント側の資格証明書をセキュリティ保護する方法３００の流れ図の一例を示している。その方法３００を、図２Ａに示すクライアント・コンピュータ・システムとサーバ・コンピュータ・システムに関して説明する。方法３００は、第１の要求をサーバに送信する動作（動作３０１）を含む。動作３０１は、クライアント・コンピュータ・システムが、サーバのリソース（例えば、電子メール・メッセージ）へのウェブ・ベースのアクセスを求める第１の要求を送信することを含むことができる。

【００５０】

例えば、クライアント・コンピュータ・システム２０１は、メール・サーバのＵＲＩ２６７を含む要求２５１をサーバ・コンピュータ・システム２１１に送信することができる。メール・サーバのＵＲＩ２６７は、電子メール・サーバ２１２に対応するＵＲＩであってよい。すなわち、電子メール・サーバが保持している電子メール・リソースにアクセスすることを望むユーザは、メール・サーバのＵＲＩ２６７にアクセスすることによって電子メール・リソースへのウェブ・ベースのアクセスを試みることができる。したがって、クライアント・コンピュータ・システム２０１のユーザは、クライアント・コンピュータ・システム２０１に要求２５１を送信させるようブラウザ２０２にコマンドを入力する。

【００５１】

方法３００は、第１の要求をクライアントから受信する動作（動作３０６）を含む。動作３０６は、サーバ・コンピュータ・システムが、サーバのリソース（例えば、電子メール・メッセージ）へのウェブ・ベースのアクセスを求める第１の要求を受信することを含むことができる。例えば、サーバ・コンピュータ・システム２１１は、メール・サーバのＵＲＩ２６７を含む要求２５１をクライアント・コンピュータ・システム２０１から受信することができる。通信フィルタ２４３を通過する破線で示すように、通信フィルタ２４

３は要求２５１を変更せずに通過させることができるよう構成することができる。この結果、要求２５１は修正なしに電子メール・サーバ２１２に転送することができる。

【００５２】

方法３００は、クライアント側の資格証明書をセキュリティ保護する機能結果志向（functional result-oriented）のステップ（ステップ３１１）を含む。ステップ３１１は、クライアント側の資格証明書をセキュリティ保護するすべての対応する動作をも含むことができる。しかし図３に示す例では、ステップ３１１は、第１の要求に呼応してクライアントをログイン・ページにリダイレクトする対応する動作（動作３０７）を含む。動作３０７は、第１の要求に呼応してサーバ・コンピュータ・システムがクライアント・コンピュータ・システムをログイン・ページにリダイレクトすることを含むことができる。

【００５３】

要求２５１に呼応して、電子メール・サーバ２１２は、無許可インジケータ２７２を含む応答（レスポンス）２５２を送信することができる。応答２５２は、ユーザの資格証明書を含んでいない要求２５１の結果として返信されたステータス・コード４０１「無許可」を有するＨＴＴＰメッセージであってよい。通信フィルタ２４３は、無許可インジケータを含むメッセージをインターセプトするように構成することができる。この結果、通信フィルタ２４３は応答２５２をインターセプトすることができる。

【００５４】

通信フィルタ２４３は、クライアント・コンピュータ・システム２０１を、ユーザの資格証明書を入力するためのインターフェースを提供するログイン・ページにリダイレクトさせるために、応答２５２のコンテンツを（例えば、ＨＴＴＰヘッダーを変更することによって）修正することができる。例えば、通信フィルタ２４３は、応答２５２から無許可インジケータ２７２を除去し、ログイン・ページのＵＲＩ２６３とリダイレクト・インジケータ２７１を応答２５２に挿入することができ、これにより応答２５２Ａが生じる。応答２５２Ａは、ステータス・コード３０２「発見」を有するＨＴＴＰメッセージであってよい。ログイン・ページのＵＲＩ２６３は、ログイン・ページ２７１にアクセスするために使用されるＵＲＩであってよい。この結果、応答２５２Ａは、要求されたリソース（例えば、電子メール・メッセージ）の代わりにログイン・ページのＵＲＩ２６３にアクセスされるということをクライアント・コンピュータ・システム２０１に示すことができる。

【００５５】

方法３００は、ログイン・ページにリダイレクトされる動作（動作（act）３０２）を含む。動作（act）３０２は、クライアント・コンピュータ・システムが、ユーザの資格証明書を受け入れるためのインターフェースを提供するログイン・ページにリダイレクトされることを含むことができる。例えば、クライアント・コンピュータ・システム２０１はログイン・ページ２１７にリダイレクトすることができる。要求２５２Ａの受信に呼応して、クライアント・コンピュータ・システム２０１は、ログイン・ページのＵＲＩ２６３を含む要求（リクエスト）２５７をサーバ・コンピュータ・システム２１１に送信することができる。要求２５７に呼応して、サーバ・コンピュータ・システム２１１は、ログイン・ページ２１７を含む応答（レスポンス）２５８をクライアント・コンピュータ・システム２０１に送信することができる。ログイン・ページは、例えばアクティブ・サーバ・ページ（「ＡＳＰ」）ページのようなウェブ・ページであってよい。

【００５６】

ブラウザ２０２はクライアント・コンピュータ・システム２０１でログイン・ページ２１７を提示することができる。図３から移動して次に図６を参照すると、図６は、本発明の原理により、ユーザの資格証明書と通信プロパティの選択を受け入れることのできるログイン・ページの一例６００を示している。ログイン・ページ２１７はログイン・ページ６００に類似していてよい。ログイン・ページ６００は、ユーザＩＤを受け入れることのできるフィールド６０６と、対応するパスワードを受諾することのできるフィールド６０７、を含む。

【００５７】

クライアント側のブラウザが「上級のクライアント」であることを示す通信プロパティ選択を受け入れるためにラジオ・ボタン６０１を使用することができる。クライアント側のブラウザが「ダウン・レベル・クライアント」であることを示す通信プロパティ選択を受け入れるためにラジオ・ボタン６０２を使用することができる。上級クライアントは、例えばスクリプトを実行すること、またはマルチメディア出力を提示することのようなさらに高度な処理を実行する機能を含むことができる。一方、ダウン・レベル・クライアントは、高度な処理を実行する機能を含むことはできない。この結果、サーバから返信されたコンテンツの豊かさは、クライアント側のブラウザの機能に応じて適切に調整することができる。上級クライアントが短縮された帯域幅および／または長い待ち時間接続（例えば、ダイヤルアップ接続）を介してサーバに接続されている場合、ダウン・レベル・クライアントの選択はサーバから返信されるコンテンツ量を低減することができる。

【００５８】

クライアント側のブラウザが「信頼のない（非信頼の）クライアント・コンピュータ・システム」であることを示す通信プロパティ選択を受け入れるために、ラジオ・ボタン６０３を使用することができる。クライアント側のブラウザが「プライベート・クライアント・コンピュータ・システム」にあることを示す通信プロパティ選択を受け入れるために、ラジオ・ボタン６０４を使用することができる。プライベート・クライアント・コンピュータ・システムは、公共アクセス（public access）が限定された（あるいはまったくない）家庭用または企業用のクライアント・コンピュータ・システムであってよい。「信頼のないクライアント・コンピュータ・システム」は、例えばホテルまたは空港のインターネット・キオスクのようなさらに多くの公共アクセスを有するクライアント・コンピュータ・システムであってよい。この結果、サーバから返信されたコンテンツに関連付けられたセキュリティは、クライアント・コンピュータ・システムの信頼性に応じて適切に調整することができる。入力されたユーザの資格証明書と選択された通信プロパティをサーバ・コンピュータ・システムに送信するためにボタン６０８を選択することができる。

【００５９】

図６から移動して次に図５を参照すると、図５は、本発明の原理により、クライアントに関連付けられた通信プロパティを決定するための方法５００の流れ図の一例を示している。方法５００を、ネットワーク・アーキテクチャ２００に示すクライアント・コンピュータ・システムとサーバ・コンピュータ・システムに関して示す。方法５００は、ログイン・ページをクライアントに送信する動作（act）（動作（act）５０１）を含む。動作５０１は、サーバ・コンピュータ・システムが、ＨＴＴＰメッセージの処理方法を変更することができる１つまたは複数の通信プロパティを選択するためのインターフェースを含むログイン・ページを送信することを含むことができる。例えば、サーバ・コンピュータ・システム２１１は、ログイン・ページ６００（または類似のログインページ）をクライアント・コンピュータ・システム２０１に送信することができる。

【００６０】

方法５００は、サーバからログイン・ページを受信する動作（動作５０５）を含む。動作５００は、クライアント・コンピュータ・システムが、サーバによるＨＴＴＰメッセージの処理方法を変更することができる１つまたは複数の通信プロパティを選択するためのインターフェースを含むログイン・ページを受信することを含むことができる。例えば、クライアント・コンピュータ・システム２０１はログイン・ページ６００（または類似のログインページ）を受信することができる。方法５００は、クライアントでログイン・ページを提示する動作（動作５０６）を含む。動作５０６は、クライアント・コンピュータ・システムのブラウザがクライアント・コンピュータ・システムでログイン・ページを提示することを含むことができる。例えば、ブラウザ２０２は、クライアント・コンピュータ・システム２０１でログイン・ページ６００（または類似のログイン・ページ）を提示することができる。

【００６１】

方法５００は、１つまたは複数の通信プロパティの少なくとも１つで選択を受信する動

作（動作５０７）を含む。動作５０７は、クライアント・コンピュータ・システムが、ログイン・ページで１つまたは複数の通信プロパティの少なくとも１つの選択を受け取ることを含むことができる。例えば、ユーザはクライアント・コンピュータ・システム２０１で、ログイン・ページ６００に通信プロパティ選択を入力するために入力装置（例えば、キーボードおよび／またはマウス）を操作することができる。ログイン・ページ６００は、ユーザが入力した選択を受け取ることができる。例えば、ログイン・ページ６００は、ラジオ・ボタン６０１またはラジオ・ボタン６０２のユーザが入力した選択、およびラジオ・ボタン６０３またはラジオ・ボタン６０４のユーザが入力した選択を受け取ることができる（場合によっては、フィールド６０６および６０７でユーザが入力した資格証明書の受け取りと共に）。

【００６２】

方法５００は、サーバの通信フィルタに通信プロパティ選択を送信する動作（動作５０８）を含む。動作５０８は、クライアント・コンピュータ・システムが、サーバ・コンピュータ・システムの通信フィルタに通信プロパティ選択を送信することを含むことができる。例えば、クライアント・コンピュータ・システム２０１は、サーバ・コンピュータ・システム２１１に通信プロパティ選択（例えば、ユーザが入力した資格証明書と共に）を送信することができる。方法５００は、クライアントから少なくとも１つの通信プロパティ選択を受信する動作（動作５０２）を含む。動作５０２は、サーバ・コンピュータ・システムがログイン・ページから選択可能な１つまたは複数の選択可能な通信プロパティの少なくとも１つの選択を受信することを含むことができる。例えば、通信フィルタ２４３は、クライアント・コンピュータ・システム２０１から（例えば、ログイン・ページ６００で選択された）１つまたは複数の通信プロパティ選択を受信することができる。

【００６３】

方法５００は、受信した少なくとも１つの通信プロパティ選択がサポートされているか否かを判定するために、またクライアントがサポートする他の関連通信プロパティを特定するために、クライアントに問い合わせる動作（動作５０３）を含む。動作５０３は、サーバ・コンピュータ・システムが、受信した通信プロパティ選択がサポートされているか否かを判定するため、またクライアントがサポートする他の関連通信プロパティを特定するために、クライアント・コンピュータ・システムに問い合わせることを含むことができる。例えば、サーバ・コンピュータ・システムは、ユーザーエージェントのＨＴＴＰヘッダーとクライアント・コンピュータ・システムの以前の知識を使用してクライアント・コンピュータ・システムの機能を決定することができる。クライアント・コンピュータ・システムの追加の機能は、ログイン・ページを介して、またクライアント・コンピュータ・システムのログイン・ページ内で実行されているスクリプト（例えば、Ｊａｖａ（登録商標）Ｓｃｒｉｐｔのスクリプト）から、決定することができる。

【００６４】

別法として、クライアント・コンピュータ・システムに対する問い合わせは、クライアント・コンピュータ・システムに構成情報をサーバ・コンピュータ・システムに対して明らかにさせる要求をクライアント・コンピュータ・システムに送信することを含むことができる。例えば、サーバ・コンピュータ・システム２１１は、ブラウザ２０２の構成を求める要求をクライアント・コンピュータ・システム２０１に送信することができる。これに呼応して、ブラウザ２０２は、例えば、バージョン番号とブラウザ２０２がｇｚｉｐ圧縮のようなＨＴＴＰ圧縮をサポートするか否かのような構成情報を示すことができる。バージョン番号に基づいて、サーバ・コンピュータ・システム２１１は、ログイン・ページ６００での「上級クライアント」の選択が適切であったか否かを判定することができる。例えば、サーバ・コンピュータ・システムは、ブラウザ２０２のバージョンがスクリプトをサポートしないと判定することができる場合がある。したがって、「上級クライアント」が選択された場合でも、サーバ・コンピュータ・システムは、簡素化したコンテンツをクライアント・コンピュータ・システム２０１に提供することができる。

【００６５】

コンテンツを簡素化することは、クライアント・コンピュータ・システムに配信されるコンテンツの量を低減することを含むことができる。例えば、ヘルプ情報に対するダウン・レベル・クライアント要求に呼応して、サーバ・コンピュータ・システムは、縮小した（冗長でない）ヘルプ情報を返信することができる。一方、ヘルプ情報に対する上級クライアント要求に呼応して、サーバ・コンピュータ・システムは、より充実させたヘルプ情報、例えば、検索スクリプトおよび他の拡張機能を含む情報を返信することができる。サーバ・コンピュータ・システムは、クライアント・コンピュータ・システムの信頼性に基づいて配信されたコンテンツを変更することができる。例えば、サーバ・コンピュータ・システムは、機密に関わる企業データへのアクセス方法に関するヘルプ情報をプライベート・クライアント・コンピュータシステムに提供することができるが、同じ情報を信頼のないクライアント・コンピュータ・システムには提供することができない。

【００６６】

サーバ・コンピュータ・システム２１１は、知らされた機能が適切にサポートされていることを検証するためにブラウザ２０２をテストする場合がある。例えば、ブラウザ２０２がｇｚｉｐ圧縮に対するサポートを示す場合、サーバ・コンピュータ・システム２１１は、ブラウザ２０２がｇｚｉｐ圧縮コンテンツを適切に処理するか否かを判定するためにｇｚｉｐ圧縮コンテンツをクライアント・コンピュータ・システム２０１に送信することができる。クライアント・コンピュータ・システム２０１が、ｇｚｉｐ圧縮に対するサポートを指示する適切な要求ヘッダーを構成することがあってよい。クライアント・コンピュータ・システム２０１は、サーバ・コンピュータ・システム２１１へ送信され／サーバ・コンピュータ・システム２１１で受信されるクライアント要求に、適切な要求ヘッダーを含めることができる。これに呼応して、サーバ・コンピュータ・システム２１１は、クライアント・コンピュータ・システム２０１がｇｚｉｐ圧縮したコンテンツを適切にキャッシュして、ウェブ・ベースのアプリケーションのセキュリティと保全性（integrity）を害さない方法でｇｚｉｐ圧縮したコンテンツを処理するか否かを判定するために、クライアント・コンピュータ・システムに問い合わせすることができる。

【００６７】

方法５００は、選択され、特定された通信プロパティに従って通信フィルタを構成する動作（動作５０４）を含む。動作５０４は、サーバ・コンピュータ・システムが、任意の選択された通信プロパティとクライアントがサポートするものであると特定された他の関連プロパティに従ってクライアントとのＨＴＴＰ通信を処理するよう通信フィルタを構成することを含むことができる。例えば、サーバ・コンピュータ・システム２１１は、ブラウザ２０２の通信プロパティ選択（例えば、上級クライアントおよび信頼のないクライアント・コンピュータ・システム）と特定された他の関連通信プロパティ（例えば、ＨＴＴＰ圧縮サポート）に従ってクライアント・コンピュータ・システム２０１とのＨＴＴＰ通信を処理するように通信フィルタ２４３を構成することができる。

【００６８】

ＨＴＴＰメッセージがサーバ・コンピュータ・システム２１１からクライアント・コンピュータ・システム２０１に送信される場合、通信フィルタ２４３は、コンテンツがクライアント・コンピュータ・システム２０１の通信プロパティに準拠するようにＨＴＴＰメッセージ・ヘッダーとＨＴＴＰメッセージのコンテンツを変更することができる。例えば、電子メール・サーバ２１２が圧縮されていない電子メール情報を有するメッセージをクライアント・コンピュータ・システム２０１に送信する場合、通信フィルタ２４３は、メッセージをインターセプトし、コンテンツをｇｚｉｐ圧縮し、その電子メール情報がｇｚｉｐ圧縮されていることを示すようにメッセージ・ヘッダーを変更することができる。別法として、例えば、インターネット情報サーバ（「ＩＩＳ」）のモジュールのようなサーバ・コンピュータ・システムの他のモジュールは、ｇｚｉｐ圧縮を実装することができる。この結果、コンテンツを、クライアント・コンピュータ・システムの機能を最大限に活用し、ユーザの望みに従うように、クライアント・コンピュータ・システムで提示することができる。

【００６９】
サーバ・コンピュータ・システム２１１が、クライアント側のブラウザが「プライベート・クライアント・コンピュータ・システム」にあることを指示する選択を受信する場合、ユーザの資格証明書をセキュリティ保護するために、例えばプライベート鍵ストア２３１のようなプライベート循環鍵ストアを使用することができる。一方、サーバ・コンピュータ・システム２１１が、クライアント側のブラウザが「信頼のないクライアント・コンピュータ・システム」にあることを指示する選択を受信する場合、ユーザの資格証明書をセキュリティ保護するために、信頼のない鍵ストア２２１のような信頼のない循環鍵ストアを使用することができる。

【００７０】
次に再び図３を参照すると、方法３００は、資格証明書をサーバに提出するためにログイン・ページを使用する動作（動作３０３）を含む。動作３０３は、クライアント・コンピュータ・システムが、資格証明書をサーバ・コンピュータ・システムに提出するためにログイン・ページを使用することを含むことができる。例えば、クライアント・コンピュータ・システム２０１は、資格証明書を（場合によっては、通信プロパティ選択と共に）サーバ・コンピュータ・システム２１１に提出するためにログイン・ページ２１７を使用することができる。ユーザの資格証明書と通信プロパティ選択を、ログイン要素のフォーマット・バリデータ（format validator）に提出されるポスト・メッセージにログイン要素として含めることができる。例えば、クライアント・コンピュータ・システム２０１は、ログイン要素２７３を含むポスト・メッセージ２５４をサーバ・コンピュータ・システムに送信することができる。

【００７１】
方法３００は、ログイン・ページで提出されたユーザの資格証明書を受信する動作（動作３０８）を含む。動作３０８は、サーバ・コンピュータ・システムが、ログイン・ページで提出されたユーザの資格証明書を受信することを含むことができる。例えば、サーバ・コンピュータ・システム２１１は、クライアント・コンピュータ・システム２０１から（場合によっては、通信プロパティ選択と共に）ユーザの資格証明書を受信することができる。資格証明書と通信プロパティ選択は、ポスト・メッセージでログイン要素として受信することができる。例えば、サーバ・コンピュータ・システム２１１は、ログイン要素２７３を含むポスト・メッセージ２５４をクライアント・コンピュータ・システム２０１から受信することができる。通信フィルタ２４３を通過する破線で示すように、通信フィルタ２４３を、ポスト・メッセージ２５４を変更せずにポスト・メッセージ２５４を通過させることができるように構成することができる。この結果、ポスト・メッセージ２５４を、修正なしにログイン要素バリデータ２１６に転送することができる。その修正の可能性、悪質な処理またはパケットに対するユーザの「スニッフィング（sniffing）」を低減し、また媒介者攻撃の可能性を低減するために、例えばトランスポート・レイヤ・セキュリティ（「ＴＬＳ」）またはセキュア・ソケット・レイヤ（「ＳＳＬ」）を使用した相互に認証された接続を、適宜、クライアント・コンピュータ・システムとサーバ・コンピュータ・システムの間に設定することができる。

【００７２】
ログイン要素バリデータ（検証器）２１６は、クライアント・コンピュータ・システム２０１に対する例えばグローバル一意識別子（「ＧＵＩＤ」）のような一意識別子を生成することもできる。ログイン要素バリデータ２１６は、受信したユーザの資格証明書（例えば、ログイン要素２７３に含まれる）をセキュリティ保護するために、デジタル署名と暗号アルゴリズムを使用することができる。例えば、ログイン要素バリデータ２１６は、受信したユーザの資格証明書の有効性を引き続いて確認するのに使用されるデジタル署名を生成することができる。ログイン要素バリデータ２１６は、循環鍵ストアの最新の鍵と生成された一意識別子と第１の定数列との組み合わせを（例えば、ＳＨＡ－１またはＭＤ－５ハッシング・アルゴリズムを使用して）ハッシュすることにより、データにデジタル署名するために使用することのできる署名鍵を導出することができる。いくつかの実施形

態では、デジタル署名はハッシュ・メッセージ認証コードとして表される。したがって、次の式１によって署名鍵を導出することができる。

K_{SIG}＝ＳＨＡ－１（$K_{MOST\ CURRENT\ ROTATING}$、ＧＵＩＤ、ＨＭＡＣＫｅｙＳｔｒｉｎｇ）・・・式１

【００７３】

式１で、$K_{MOST\ CURRENT\ ROTATING}$は、適切な循環鍵ストアの最新の鍵を表している。例えば、ブラウザ２０２が（例えば、通信プロパティ選択によって指示されるように）「プライベート・クライアント・コンピュータ・システム」にある場合、$K_{MOST\ CURRENT\ ROTATING}$はプライベート循環鍵ストア２３１の最新の鍵（例えば、鍵２３２）を表す。ＧＵＩＤは、クライアント・コンピュータ・システム２０１に対応する一意識別子を表す。ＨＭＡＣＫｅｙＳｔｒｉｎｇは、テキストの定数列を表す。次の式２によってK_{SIG}からハッシュ・メッセージ認証コードを生成することができる。

デジタル署名＝ＨＭＡＣ（K_{SIG}、（ＧＵＩＤ、｛ユーザ名：パスワード｝、フラグ））・・・式２

【００７４】

式２で、ＨＭＡＣは、例えばＲｅｑｕｅｓｔ Ｆｏｒ Ｃｏｍｍｅｎｔｓ（「ＲＦＣ」）２１０４に記載のようなハッシュ・メッセージ認証コード・アルゴリズムを表す。式２の（ＧＵＩＤ、｛ユーザ名：パスワード｝、フラグ）部分は、ＧＵＩＤとユーザの資格証明書と通信プロパティ選択がハッシュ・メッセージ認証コード・アルゴリズムに入力されるテキストとして含まれることを表すフラグとを表す。ユーザの資格証明書を、適宜、ハッシュ・メッセージ認証コード・アルゴリズムに準拠させるためにテキスト形式に（例えば、ユーザの資格証明書をｂｅｓｅ６４符号化することによって）変換することができる。ハッシュ・メッセージ認証コード・アルゴリズムに関して説明したが、デジタル署名を生成するために使用されるアルゴリズムは重要ではなく、事実上いかなるデジタル署名、ダイジェスト、または認証コード・アルゴリズムを使用することもできる。

【００７５】

ログイン要素バリデータ２１６は、循環鍵ストアの最新の鍵と一意識別子と第２の定数列との組み合わせをハッシュすることによって、データを暗号化するために使用することのできる暗号鍵を導出することもできる。したがって、次の式３によって暗号鍵を導出することができる。

K_{ENC}＝ＳＨＡ－１（$K_{MOST\ CURRENT\ ROTATING}$、ＧＵＩＤ、ＥｎｃｒｙｐｔＫｅｙＳｔｉｒｎｇ）・・・式３

【００７６】

式３で、$K_{MOST\ CURRENT\ ROTATING}$は、署名鍵を生成する際に使用された循環鍵ストアからの最新の鍵を表す。したがって、K_{SIG}を生成するために鍵２３２が使用された場合、鍵２３２はK_{ENC}を生成するためにも使用することができる。ＧＵＩＤは、クライアント・コンピュータ・システム２０１に対応する一意識別子を表す。ＥｎｃｒｙｐｔＫｅｙＳｔｒｉｎｇは、ＨＭＡＣＫｅｙＳｔｒｉｎｇとは異なるテキストの定数列を表す。したがって、次の式４によって暗号化された情報を生成することができる。

暗号化された情報＝K_{ENC}［デジタル署名、｛ユーザ名：パスワード｝、フラグ］・・・式４

【００７７】

式４では、デジタル署名は、式２によって生成されたデジタル署名を表し、｛ユーザ名：パスワード｝はユーザの資格証明書を表し、フラグは通信プロパティ選択を表す。

【００７８】

ステップ３１１は、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号化された情報を送信する対応する動作（動作３０９）を含む。動作３０９は、サーバ・コンピュータ・システムが、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号

化された情報をクライアント・コンピュータ・システムに送信することを含むことができる。例えば、ログイン要素バリデータ２１６は、ＧＵＩＤ２７４および暗号化された資格証明書２７５を含むメッセージ２５５をクライアント・コンピュータ・システム２０１に送信することができる。通信フィルタ２４３を通過する破線で示すように、通信フィルタ２４３を、メッセージ２５５を変更せずに通過させるように構成することができる。したがって、メッセージ２５５を修正なしにクライアント・コンピュータ・システム２０１に転送することができる。

【００７９】

方法３００は、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号化された情報を受信する動作（動作３０４）を含む。動作３０４は、クライアント・コンピュータ・システムが、ユーザの資格証明書の少なくとも一部と時間依存署名を表す暗号化された情報をサーバ・コンピュータ・システムから受信することを含むことができる。例えば、クライアント・コンピュータ・システム２０１は、ＧＵＩＤ２７４と暗号化された資格証明書２７５を含むメッセージ２５５をサーバ・コンピュータ・システム２１１から受信することができる。クライアント・コンピュータ・システム２０１がＧＵＩＤ２７４と暗号化された資格証明書２７５をクッキー２０３に記憶するように、メッセージ２５５を構成することができる。例えば、メッセージ２５５は次のように構成することができる。

Ｓｅｔ－Ｃｏｏｋｉｅ：ｓｅｓｓｉｏｎｉｄ＝｛ＧＵＩＤ｝；パス＝／

Ｓｅｔ－Ｃｏｏｋｉｅ：ｃｒｅｄｄａｔａ＝｛暗号化された情報｝；パス＝／

【００８０】

方法３００は、暗号化された情報を含む第２の要求を送信する動作（動作３０５）を含む。動作３０５は、クライアント・コンピュータ・システムが、リソース（例えば、第１の要求で要求された電子メール・メッセージ）へのウェブ・ベースのアクセスを求める第２の要求を送信することを含むことができる。例えば、クライアント・コンピュータ・システム２０１は、メール・サーバのＵＲＩ２６７とＧＵＩＤ２７４と暗号化された資格証明書２７５とを含む要求２５６をサーバ・コンピュータ・システム２１１に送信することができる。方法３００は、暗号化された情報を含む第２の要求を受信する動作（動作３１０）を含む。動作３１０は、サーバ・コンピュータ・システムが、リソース（例えば、第１の要求で要求された電子メール・メッセージ）へのウェブ・ベースのアクセスを求める第２の要求を受信することを含むことができる。例えば、サーバ・コンピュータ・システム２１１は、メール・サーバのＵＲＩ２６７とＧＵＩＤ２７４と暗号化された資格証明書２７５とを含む要求２５６をクライアント・コンピュータ・システム２０１から受信することができる。

【００８１】

いくつかの実施形態では、クライアント・コンピュータ・システムは、ＧＵＩＤと暗号化された情報を有する対応するクッキーをブラウザ・メモリに既に記憶している。この記憶されているＧＵＩＤと暗号化された情報とを、サーバのリソース（例えば、電子メールのデータ）へのウェブ・ベースのアクセスを要求する場合に、使用することができる。図２Ｂは、本発明により、サーバのリソースにアクセスするためにセキュリティ保護されたクライアント側の資格証明書を使用することに役立つネットワーク・アーキテクチャ２００の一例を示している。図４は、本発明による、セキュリティ保護されたクライアント側の資格証明書をサーバのリソースへのアクセスに使用することを容易にする方法４００の流れ図の一例を示している。方法４００を、図２Ｂに示すクライアント・コンピュータ・システムとサーバ・コンピュータ・システムに関して説明する。

【００８２】

図４００は、サーバのリソースへのウェブ・ベースのアクセスを求める、セッションＩＤと暗号化されたユーザの資格証明書を含む、要求を送信する動作（動作４０１）を含む。動作４０１は、クライアント・コンピュータ・システムが、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を送信することを含むことができる。例えば、クライアント・コンピュータ・システム２０１は、メール・サーバの

ＵＲＩ２６７とＧＵＩＤ２７４と暗号化された資格証明書２７５とを含む要求（リクエスト）２９１をサーバ・コンピュータ・システム２１１に送信することができる。メール・サーバのＵＲＩ２６７は、電子メール・サーバ２１２によって制御されている電子メール・リソースへのアクセスを提供するＵＲＩを表す。ＧＵＩＤ２７４は、以前にサーバ・コンピュータ・システム２１１からクライアント・コンピュータ・システム２０１に送信された一意のセッションＩＤを表す。暗号化された資格証明書２７５は、以前にサーバ・コンピュータ・システム２１１からクライアント・コンピュータ・システム２０１に送信された暗号化されたユーザの資格証明書と時間依存署名とを表す。暗号化された資格証明書２７５は、適切な循環鍵ストアの鍵から既に生成済みである。

【００８３】

方法４００は、サーバのリソースへのウェブ・ベースのアクセスを求める、セッションＩＤと暗号化されたユーザの資格証明書とを含む要求を受信する動作（動作４０４）を含む。動作４０４は、サーバ・コンピュータ・システムが、サーバ・コンピュータ・システムのリソースへのウェブ・ベースのアクセスを求める要求を受信することを含むことができる。例えば、サーバ・コンピュータ・システム２１１は、メール・サーバのＵＲＩ２６７とＧＵＩＤ２７４と暗号化された資格証明書２７５とを含む要求２９１をクライアント・コンピュータ・システム２０１から受信することができる。

【００８４】

方法４００は、循環鍵ストアの最新の鍵を使用して暗号化されたユーザの資格証明書の有効性確認を試みる動作（動作４０５）を含む。動作４０５は、サーバ・コンピュータ・システムが、循環鍵ストアの最新の鍵を使用してユーザの資格証明書の少なくとも一部の有効性確認を試みることを含むことができる。例えば、ブラウザ２０２がプライベート・クライアント・コンピュータ・システムにあることが示された場合、サーバ・コンピュータ・システムは鍵２３２を使用して暗号化された資格証明書２７５の有効性確認を試みることができる。一方、ブラウザ２０２が信頼のないクライアント・コンピュータ・システムにあることが示された場合、サーバ・コンピュータ・システムは、鍵２２２を使用して暗号化された資格証明書２７５の有効性確認を試みることができる。資格証明書バリデータ２３７は、適切な循環鍵ストアの最新の鍵と一意識別子と第２の定数列（暗号鍵を導出する際に使用される）との組み合わせをハッシュすることによって、データを暗号解読するために使用される暗号解読鍵を導出することができる。したがって、次の式５によって暗号解読鍵を導出することができる。

K_{DCR}＝ＳＨＡ－１（$K_{MOST\ CURRENT\ ROTATING}$、ＧＵＩＤ、ＥｎｃｒｙｐｔＫｅｙＳｔｒｉｎｇ）・・・式５

【００８５】

式５では、$K_{MOST\ CURRENT\ ROTATING}$は適切な循環鍵ストアの最新の鍵（例えば、鍵２３２または鍵２２２）を表す。ＧＵＩＤは、クライアント・コンピュータ・システム２０１に対応する一意識別子を表す。ＥｎｃｒｙｐｔＫｅｙＳｔｒｉｎｇは、K_{ENC}の導出中に使用される定数列を表す。したがって、資格証明書バリデータ２３７は、次の式６によって、デジタル署名とユーザの資格証明書と通信プロパティ選択を表すフラグとを明らかにするために暗号化された情報を暗号解読することができる。

デジタル署名、｛ユーザ名：パスワード｝、フラグ＝K_{DCR}［暗号化された情報］・・・式６

【００８６】

資格証明書バリデータ２３７は、適切な循環鍵ストアの最新の鍵と一意識別子と第１の定数列との組み合わせをハッシュすることによって、有効性確認デジタル署名を生成するために使用することができる有効性確認鍵を導出することができる。いくつかの実施形態では、有効性確認デジタル署名はハッシュ・メッセージ認証コードとして表される。したがって、次の式７によって有効性確認鍵を導出することができる。

K_{VAL}＝ＳＨＡ－１（$K_{MOST\ CURRENT\ ROTATING}$、ＧＵＩＤ、ＨＭＡＣＫｅｙＳｔｒｉｎｇ）・・・式７

【００８７】

式７では、$K_{MOST\ CURRENT\ ROTATING}$は、適切な循環鍵ストアの最新の鍵を表す。ＧＵＩＤは、クライアント・コンピュータ・システム２０１に対応する一意識別子を表す。ＨＭＡＣＫｅｙＳｔｒｉｎｇは、署名鍵を導出する場合に使用されるテキストの定数列を表す。K_{VAL}から、また式６から明らかになったユーザの資格証明書とフラグを使用して、ハッシュ・メッセージ認証コードを次の式８によって生成することができる。

有効性確認デジタル署名＝ＨＭＡＣ（K_{VAL}、（ＧＵＩＤ、｛ユーザ名：パスワード｝、フラグ））・・・式８

【００８８】

式８では、ＨＭＡＣはハッシュ・メッセージ認証コード・アルゴリズムを表す。式８の（ＧＵＩＤ、｛ユーザ名：パスワード｝、フラグ）の部分は、ＧＵＩＤとユーザの資格証明書と通信プロパティ選択を表すフラグがハッシュ・メッセージ認証コード・アルゴリズムに入力されるテキストとして含まれていることを表す。ハッシュ・メッセージ認証コード・アルゴリズムに関して説明しているが、有効性確認デジタル署名を生成するために使用されるこのアルゴリズムは重要ではなく、事実上いかなるデジタル署名、ダイジェスト、または認証コード・アルゴリズムでも使用することができる。

【００８９】

有効性確認デジタル署名がデジタル署名と等しい場合、暗号化された資格証明書２７５で表されたユーザの資格証明書は有効であるとされる。したがって、通信フィルタ２４３は、有効であるとされたユーザの資格証明書を含む許可ヘッダー（例えば、ＨＴＴＰ許可ヘッダー）を構築する。通信フィルタ２４３は、リソースへのウェブ・ベースのアクセスを求める要求に許可ヘッダーを挿入することができる。例えば、通信フィルタ２４３は、要求２９１から暗号化された資格証明書２７５を除去し、要求２９１に資格証明書２８９を挿入することができ、この結果、要求２９１Ａが生じる。

【００９０】

有効性確認デジタル署名がデジタル署名に等しくない場合、ユーザの資格証明書は有効であるとされない。したがって、資格証明書バリデータ２３７は、適切な循環鍵ストアの次に新しい鍵に基づいて式５、６、７および８の機能を反復する。例えば、プライベート・クライアント・コンピュータ・システムのクライアント側のブラウザに対して、資格証明書バリデータ２３７は鍵２３３を使用することができる。一方、信頼のないクライアントのクライアント側のブラウザに対しては、資格証明書バリデータ２３７は鍵２２３を使用することができる。資格証明書バリデータは、適切な循環鍵ストアの各鍵を使用してユーザの資格証明書の有効性確認を試みることができる。有効であるとされたユーザの資格証明書は、適切な認証ヘッダーに含めることができる。

【００９１】

いくつかの実施形態では、暗号化された資格証明書の有効性確認を試みるために使用されるべき循環鍵（例えば、資格証明書を暗号化するために以前使用された循環）を指示するために、インデックスが、暗号化された資格証明書と共に含まれる。例えば、クライアント・コンピュータ・システム２０１は、信頼のない循環鍵ストア２２１またはプライベート循環鍵ストア２３１の循環鍵を特定するインデックスを、要求２９１に含めることができる。インデックスは、使用されるべき循環鍵の生成を特定する数値（例えば、０、１、２など）であってよい。例えば、クライアント・コンピュータ・システム２０１がプライベート・クライアント・コンピュータ・システムである場合、インデックス０は鍵２３２を特定することができる。同様に、クライアント・コンピュータ・システム２０１が信頼のないクライアント・コンピュータ・システムである場合、インデックス２は鍵２２４を特定することができる。したがって、インデックスを使用することによって有効性確認プロセスの効率が高まる。資格証明書がインデックスで特定された循環鍵によって有効であるとされない場合、対応する循環鍵ストアの他の鍵を使用して資格証明書の有効性確認を試みることができる。

【００９２】
方法４００は、要求されたリソースへのウェブ・ベースのアクセスを制御するモジュールに要求を転送する動作（動作４０６）を含む。動作４０６は、サーバ・コンピュータ・システムが、リソースへのウェブ・ベースのアクセスを制御するモジュールに要求を転送することを含むことができる。例えば、通信フィルタ２４３は、（暗号化された資格証明書２７５から明らかになるような）メール・サーバのＵＲＩ２６７と資格証明書２８９とを含む要求２９１Ａを電子メール・サーバ２１２に転送することができる。電子メール・サーバ２１２は、電子メール・リソースへのウェブ・ベースのアクセスを制御するモジュールであってよい。電子メール・サーバ２１２は、要求された電子メール・リソースへのウェブ・ベースのアクセスが許可されているか否かを判定するために資格証明書２８９を資格証明書データベース２１３と比較することができる。

【００９３】
方法４００は、リフレッシュされた暗号化されたユーザの資格証明書を循環鍵ストアの最新の鍵から導出すべきか否かを判定する動作（動作４０７）を含む。動作４０７は、サーバ・コンピュータ・システムが、ユーザの資格証明書と時間依存署名を表すリフレッシュされた暗号化された情報を循環鍵ストアの最新の鍵から導出すべきか否かを判定することを含むことができる。ユーザの資格証明書が循環鍵ストアの最新の鍵以外の鍵によって有効であるとされる場合、サーバはリフレッシュされた暗号化された情報が導出されるべきであると決定する。例えば、資格証明書バリデータ２３７が暗号化された資格証明書を鍵２２４によって有効であるとする場合、通信フィルタ２４３は、暗号化された資格証明書に表されたユーザの資格証明書に関して、リフレッシュされた暗号化された資格証明書が導出されるべきであると決定することができる。

【００９４】
したがって、破線で示したように、通信フィルタ２４３は、要素バリデータ２１６にログインするために任意選択でクッキー・リフレッシュ要求２９４を送信することができる。ログイン要素バリデータ２１６は、（例えば、最新の鍵からリフレッシュされたデジタル署名とリフレッシュされた暗号鍵を導出することによって）リフレッシュされた暗号化された情報を導出するために適切な循環鍵ストアの最新の鍵を使用することができる。ログイン要素バリデータ２１６は、更新されたＧＵＩＤとリフレッシュされた暗号化された資格証明書とを通信フィルタ２４３に返信することができる。例えば、破線で示すように、ログイン要素バリデータ２１６は、更新されたＧＵＩＤ２９６とリフレッシュされた暗号化された資格証明書２９７を含むメッセージ２９５を通信フィルタ２４３に返信する。

【００９５】
資格証明書２８９が、電子メール・サーバ２１２の電子メール・リソースへのウェブ・ベースのアクセスに適切である場合、電子メール・サーバ２１２は、要求２９１Ａに呼応して電子メール・リソースを返信することができる。例えば、電子メール・サーバ２１２は、リソース２９３（例えば、電子メール・メッセージ）を含む応答（レスポンス）２９２を通信フィルタ２４３に返信することができる。一方、資格証明書２８９が、電子メール・サーバ２１２の電子メール・リソースへのウェブ・ベースのアクセスに適切でない場合、電子メール・サーバ２１２は、要求２９１Ａに呼応して無許可であるという指示を返信することができる。例えば破線で示すように、電子メール・サーバ２１２は、無許可インジケータ２７２を含む応答（レスポンス）２９４を通信フィルタ２４３に返信することができる。通信フィルタ２４３が無許可インジケータを受信する場合、通信フィルタ２４３はクライアント・コンピュータ・システム２０１をログイン・ページ２１７にリダイレクトすることができる。

【００９６】
有効性確認されたユーザの資格証明書が適切である場合、通信フィルタ２４３は要求されたリソースをクライアント・コンピュータ・システム２０１に送信することができる。例えば、暗号化された資格証明書２７５が適切な循環鍵ストアからの最新の鍵によって有効性確認される場合、リソース２９３を含む応答２９２は通信フィルタ２４３で受信され

る。通信フィルタ２４３は、応答２９２をクライアント・コンピュータ・システム２０１に転送することができる。したがって、リソース２９３がブラウザ２０２で提示される。

【００９７】

有効性確認されたユーザの資格証明書が適切である場合、通信フィルタ２４３は、リフレッシュされた暗号化された資格証明書と更新されたＧＵＩＤもリソースと共にクライアント・コンピュータ・システム２０１に送信することができる。例えば、暗号化された資格証明書２７５が循環鍵ストアの最新の鍵ではない鍵によって有効性確認される場合、リソース２９３と更新されたＧＵＩＤ２９６とリフレッシュされた暗号化された資格証明書２９７をすべて通信フィルタ２４３で受信することができる。破線で示すように、次いで通信モジュール２４３は、リソース２９３と更新されたＧＵＩＤ２９６とリフレッシュされた暗号化された資格証明書２９７とを含む応答（レスポンス）２７６をクライアント・コンピュータ・システム２０１に送信することができる。

【００９８】

方法４００は、リソースを、更新されたセッションＩＤとリフレッシュされた暗号化されたユーザの資格証明書と共に、クライアント側のブラウザで受信する動作（動作４０２）を含む。動作４０２は、クライアント・コンピュータ・システムが、要求されたものを、更新されたセッションＩＤと、ユーザの資格証明書の少なくとも一部とリフレッシュされた時間依存署名を表すリフレッシュされた暗号化された情報と共に、受信することを含むことができる。例えば、クライアント・コンピュータ・システム２０１は、リソース２９３と更新されたＧＵＩＤ２９６とリフレッシュされた暗号化された資格証明書２９７とを含む応答２７６をサーバ・コンピュータ・システム２０１から受信することができる。

【００９９】

方法４００は、更新されたセッションＩＤとリフレッシュされた暗号化されたユーザの資格証明書を対応するクッキーに記憶する動作（動作４０３）を含む。動作４０３は、クライアント・コンピュータ・システムが、更新されたセッションＩＤとリフレッシュされた暗号化された情報をクライアント・コンピュータ・システムの対応するクッキーに記憶することを含むことができる。例えば、更新されたＧＵＩＤ２９６とリフレッシュされた暗号化された資格証明書２９７でＧＵＩＤ２７４と暗号化された資格証明書２７５を上書きして、クッキー２０３の対応するクッキーに記憶することができる。

【０１００】

本発明は、その趣旨または本質的な特性から逸脱せずに他の特定の形式で実施することができる。記載した実施形態は、すべての点で説明のみを目的としたものであり限定を目的としたものではないとみなされるべきである。したがって、本発明の範囲は上記の説明ではなく特許請求の範囲によって示される。特許請求の範囲と等価の意味および範囲内のすべての変更は、本特許請求の範囲に包含されるべきである。

【図面の簡単な説明】

【０１０１】

【図１】本発明の原理に適した動作環境を示す図である。

【図２Ａ】本発明による、クライアントがサーバのリソースへのアクセスを要求する場合にクライアント側の資格証明書をセキュリティ保護することに役立つネットワーク・アーキテクチャの一例を示す図である。

【図２Ｂ】本発明による、サーバのリソースにアクセスするためにセキュリティ保護されたクライアント側の資格証明書を使用することに役立つネットワーク・アーキテクチャの一例を示す図である。

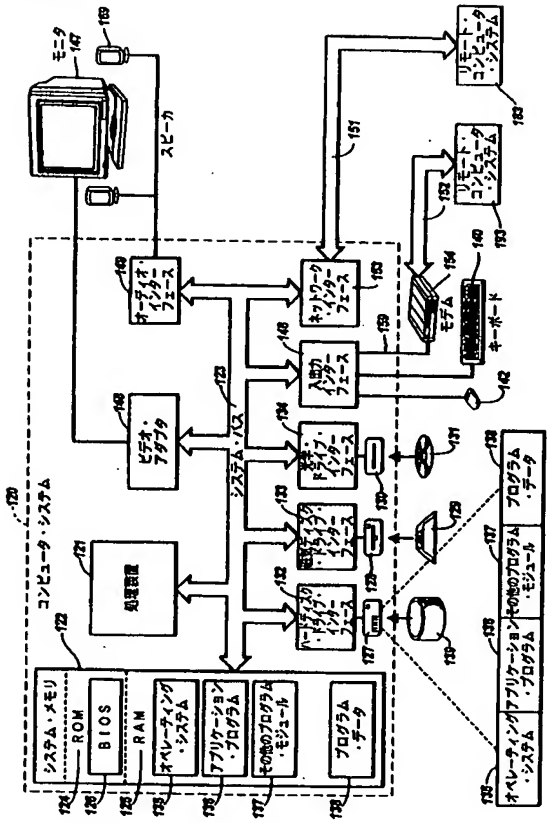
【図３】本発明による、クライアントがサーバのリソースへのアクセスを要求する場合にクライアント側の資格証明書をセキュリティ保護する方法の流れ図の一例を示す図である。

【図４】本発明による、サーバのリソースにアクセスするためにセキュリティ保護されたクライアント側の資格証明書を使用する方法の流れ図の一例を示す図である。

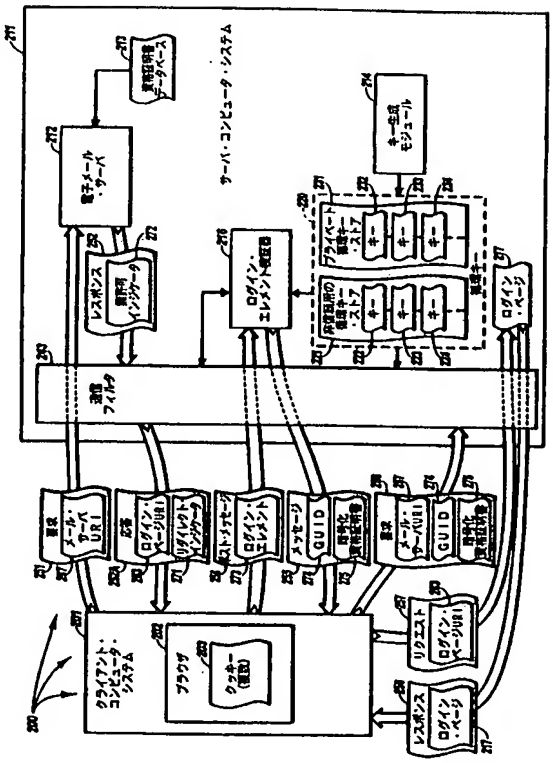
【図５】本発明の原理による、クライアントに関連付けられた通信プロパティを決定する

方法の流れ図の一例を示す図である。
【図６】本発明の原理による、資格証明書と通信プロパティ選択を受諾することができるログイン・ページの一例を示す図である。
【符号の説明】
【０１０２】
１２０　コンピュータ・システム
１２１　処理装置
１２２　システム・メモリ
１２３　システム・バス
１３２　ハードディスク・ドライブ・インターフェース
１３３　磁気ディスクドライブ・インターフェース
１３４　光ディス・クインターフェース
１３５　オペレーティング・システム
１３６　アプリケーション・プログラム
１３７　他のプログラム・モジュール
１３８　プログラム・データ
１４０　キーボード
１４６　入出力インターフェース
１４７　モニタ
１４８　ビデオ・アダプタ
１４９　音声インターフェース
１５３　ネットワーク・インターフェース
１５４　モデム
１６９　スピーカー
１８３　遠隔コンピュータ・システム
１９３　遠隔コンピュータ・システム

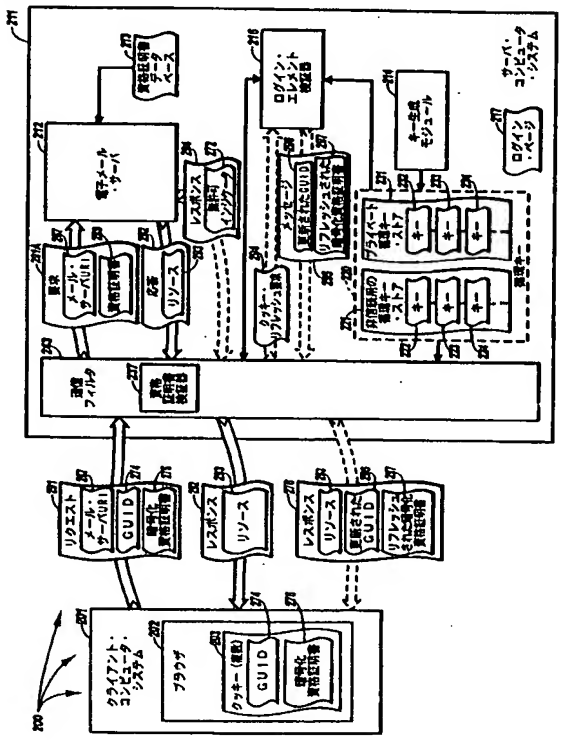
【図１】



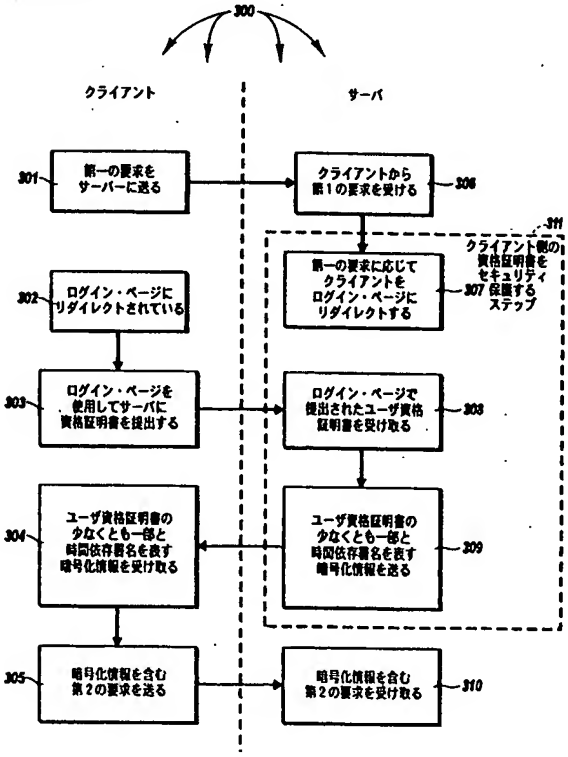
【図２Ａ】



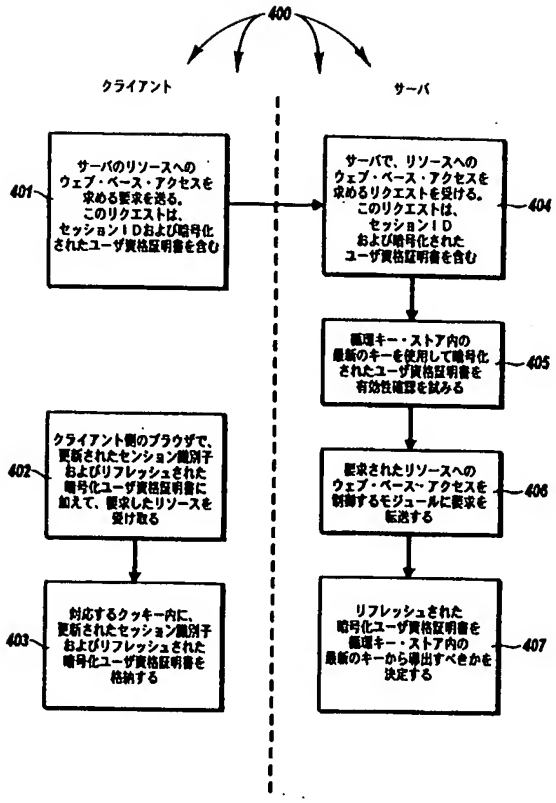
【図２Ｂ】



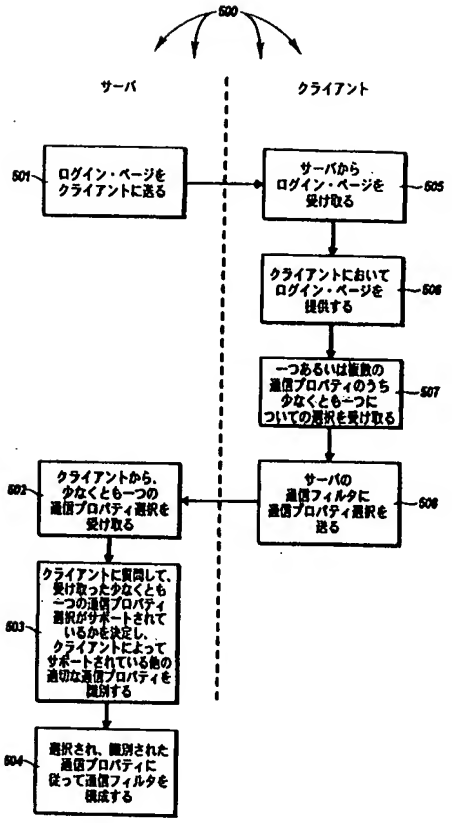
【図３】


300
クライアント
サーバ
301
第一の要求をサーバーに送る
306
クライアントから第1の要求を受ける
311
クライアント側の資格証明書をセキュリティ保護するステップ
307
第一の要求に応じてクライアントをログイン・ページにリダイレクトする
302
ログイン・ページにリダイレクトされている
303
ログイン・ページを使用してサーバに資格証明書を提出する
308
ログイン・ページで提出されたユーザ資格証明書を受け取る
304
ユーザ資格証明書の少なくとも一部と時間依存署名を表す暗号化情報を受け取る
309
ユーザ資格証明書の少なくとも一部と時間依存署名を表す暗号化情報を送る
305
暗号化情報を含む第2の要求を送る
310
暗号化情報を含む第2の要求を受け取る

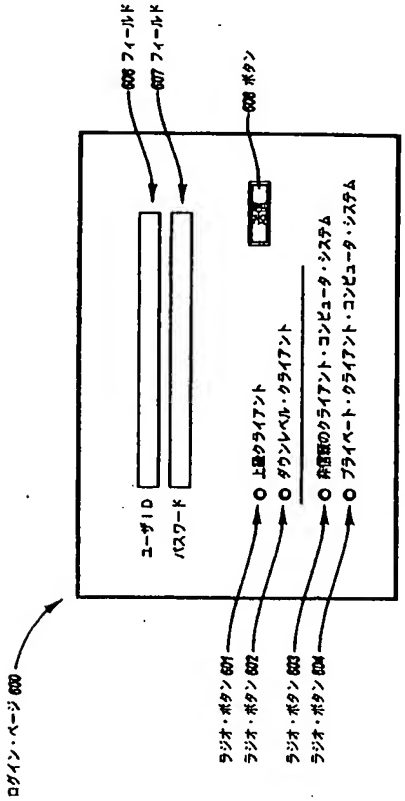
【図４】


400
クライアント
サーバ
401
サーバのリソースへのウェブ・ベース・アクセスを求める要求を送る。このリクエストは、セッションIDおよび暗号化されたユーザ資格証明書を含む
404
サーバで、リソースへのウェブ・ベース・アクセスを求めるリクエストを受ける。このリクエストは、セッションIDおよび暗号化されたユーザ資格証明書を含む
405
鍵理キー・ストア内の最新のキーを使用して暗号化されたユーザ資格証明書を有効性確認を試みる
402
クライアント側のブラウザで、更新されたセッション識別子およびリフレッシュされた暗号化ユーザ資格証明書に加えて、要求したリソースを受け取る
406
要求されたリソースへのウェブ・ベース・アクセスを制御するモジュールに要求を転送する
403
対応するクッキー内に、更新されたセッション識別子およびリフレッシュされた暗号化ユーザ資格証明書を格納する
407
リフレッシュされた暗号化ユーザ資格証明書を鍵理キー・ストア内の最新のキーから導出すべきかを決定する

【図５】


500
サーバ
クライアント
501
ログイン・ページをクライアントに送る
505
サーバからログイン・ページを受け取る
506
クライアントにおいてログイン・ページを提供する
507
一つあるいは複数の通信プロパティのうち少なくとも一つについての選択を受け取る
508
サーバの通信フィルタに通信プロパティ選択を送る
502
クライアントから、少なくとも一つの通信プロパティ選択を受け取る
503
クライアントに質問して、受け取った少なくとも一つの通信プロパティ選択がサポートされているかを決定し、クライアントによってサポートされている他の適切な通信プロパティを識別する
504
選択され、識別された通信プロパティに従って通信フィルタを構成する

【図６】


606 フィールド
607 フィールド
608 ボタン
ユーザID
パスワード
上級クライアント
ダウンレベル・クライアント
非信頼のクライアント・コンピュータ・システム
プライベート・クライアント・コンピュータ・システム
ラジオ・ボタン 601
ラジオ・ボタン 602
ラジオ・ボタン 603
ラジオ・ボタン 604
ログイン・ページ 600

フロントページの続き

(72)発明者 リチャード ビー. ウォード
アメリカ合衆国 98053 ワシントン州 レッドモンド 261 アベニュー ノースイースト 8565
(72)発明者 ラッセル リー シンプソン ジュニア
アメリカ合衆国 98034 ワシントン州 カークランド 79 プレイス ノースイースト 11136
(72)発明者 カリム ミシェル バティシュ
アメリカ合衆国 98117 ワシントン州 シアトル メイビー アベニュー ノースウエスト 9214

Fターム(参考) 5B085 AE02 AE03 AE09 BC01
5J104 AA07 AA16 AA34 EA04 EA19 JA21 KA01 KA04 LA03 NA02
NA05 NA12 NA37 NA38 PA07

【要約の続き】